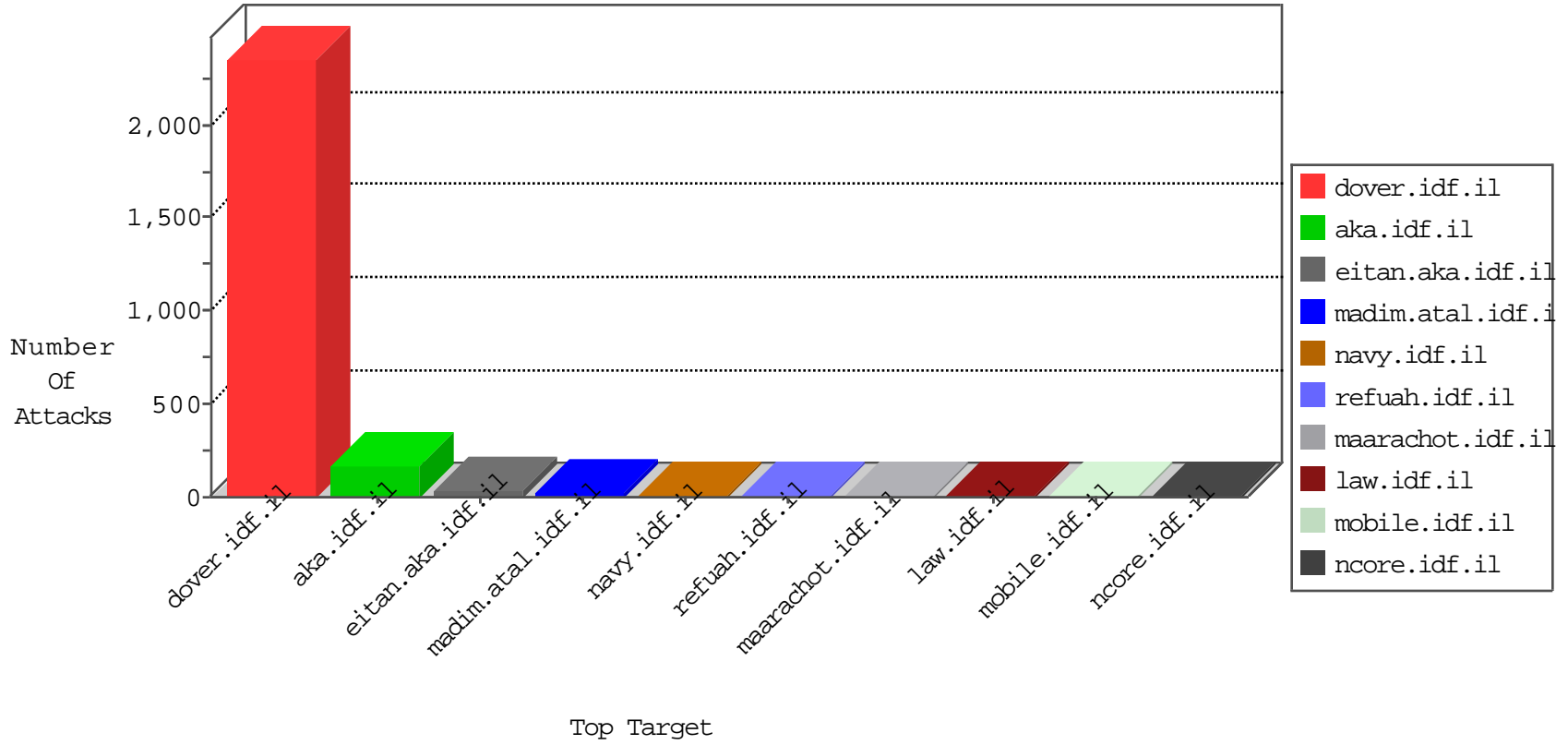


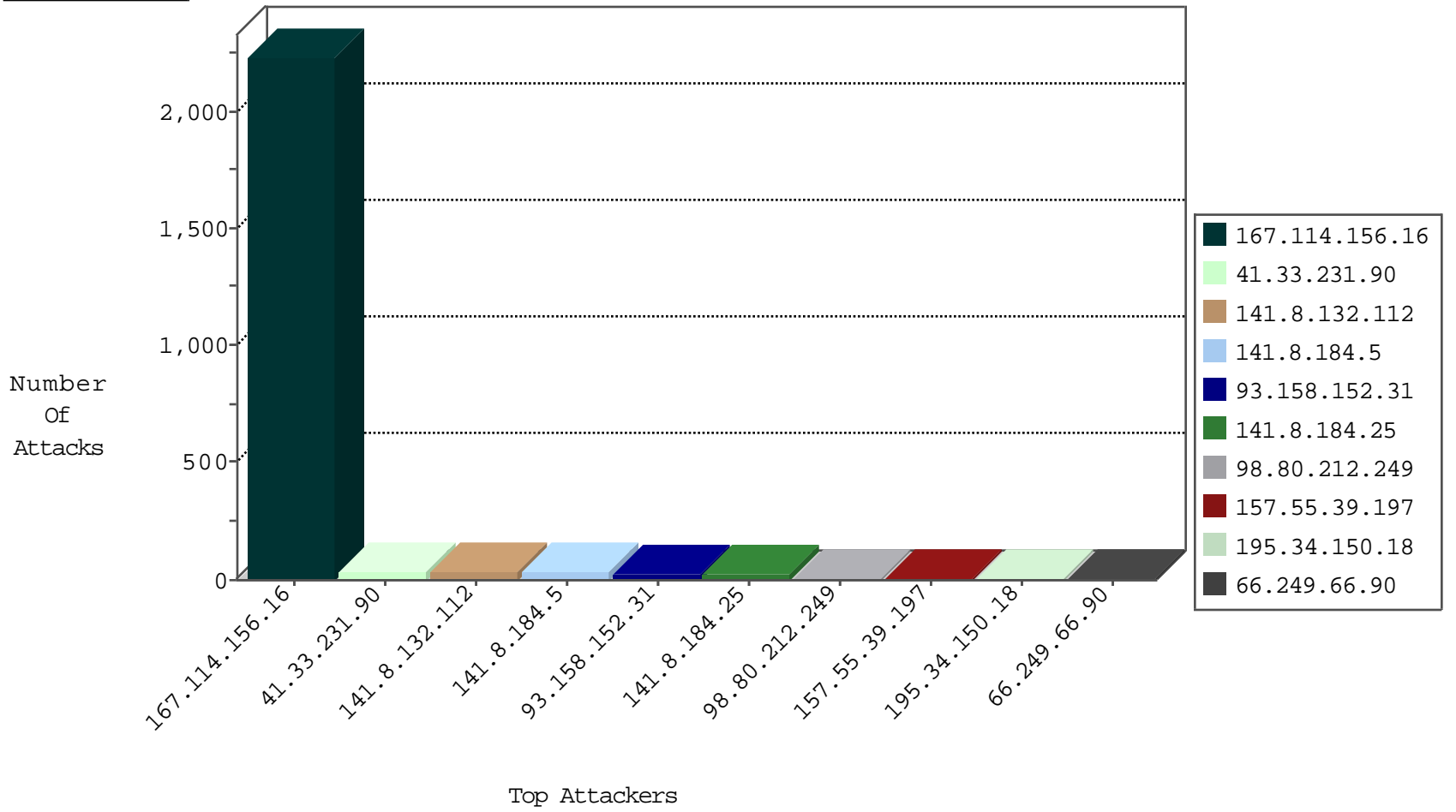
# IDF Under Attack Daily Report



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	3080
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
23.95.54.18	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.119.121.146	Ukraine	147.237.76.42	refuah.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
46.119.121.146	Ukraine	147.237.77.170	maarachot.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
182.50.130.134	Singapore	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1

## 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
183.60.48.25	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
104.37.187.183	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
85.93.5.65	147.237.77.170	Germany	maarachot.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.120	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.72.156	United States	aman.idf.il	ET DROP Dshield Block Listed Source	1
193.105.134.220	147.237.77.233	Sweden	atal.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
104.37.187.183	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -f -sS	1
46.161.40.120	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
31.155.203.162	147.237.76.30	Turkey	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.246.0.97	147.237.0.19	China	madim.atal.idf.i	ET SCAN NMAP -sS window 1024	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
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
141.8.184.5	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
93.158.152.31	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
141.8.184.25	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
207.46.13.5	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
40.77.167.105	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
157.55.39.197	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
141.8.142.62	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.163.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
98.80.212.249	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
131.253.25.177	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.86.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
98.80.212.249	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
141.8.132.8	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.255.253.96	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
147.236.238.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.65.98.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.52.2.154	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.249.66.95	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.210	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
81.169.237.146	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	2
207.46.13.108	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
149.78.219.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.65.98.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
98.80.212.249	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.182	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.158.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.29.67.86	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.54	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.92	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.39.78.130	Kuwait	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
108.168.185.133	United States	147.237.0.33	idf.il	drop		drop	1
2.52.32.228	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.10	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.232	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.253.158.175	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.115.60.112	Iran, Islamic Republic of	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
77.125.135.240	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.112	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.117.242.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
108.168.185.133	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.22.129.247	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
81.169.237.146	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.13.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
188.143.232.34	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.34	Block	5
5.29.72.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
212.116.184.161	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	4
212.116.184.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
91.143.80.201	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
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	2
80.246.136.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
176.13.8.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
74.82.47.2	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.229.164.99	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
2.54.128.226	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
79.183.219.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.79.79	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17306-en/dover.aspx-title=idf	Block	1
212.179.42.227	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1129-he/dover.aspx	Block	1
46.119.121.146	Ukraine	147.237.76.42	refuah.idf.il	Unauthorized URL Access to ww.refua.atal.idf.il/wp-login.php	Block	1
91.228.196.139	Poland	147.237.77.74	law.idf.il	PHP Attempt	Block	1
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
207.46.13.108	United States	147.237.72.166	aka.idf.il	Abnormally Long Request URL	Block	1
66.230.230.230	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.100.57.75	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
46.119.121.146	Ukraine	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
176.13.15.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
91.228.196.139	Poland	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-signup.php	Block	1
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.69.40	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2880.pdf	Block	1
37.26.147.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.212.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.118.236.13	Bulgaria	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
68.100.57.75	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
46.119.121.146	Ukraine	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
93.172.163.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.96.48	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
46.19.85.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.237	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in ww.tikshuv.idf.il/site/general.aspx	Block	1
89.247.109.64	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
68.180.228.175	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/228-he/faq.aspx	Block	1
188.143.232.34	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/homepage.aspx/templates/social/twitter.aspx	Block	1
46.229.164.99	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	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
2.52.32.224	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
79.182.96.48	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
46.119.121.146	Ukraine	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1