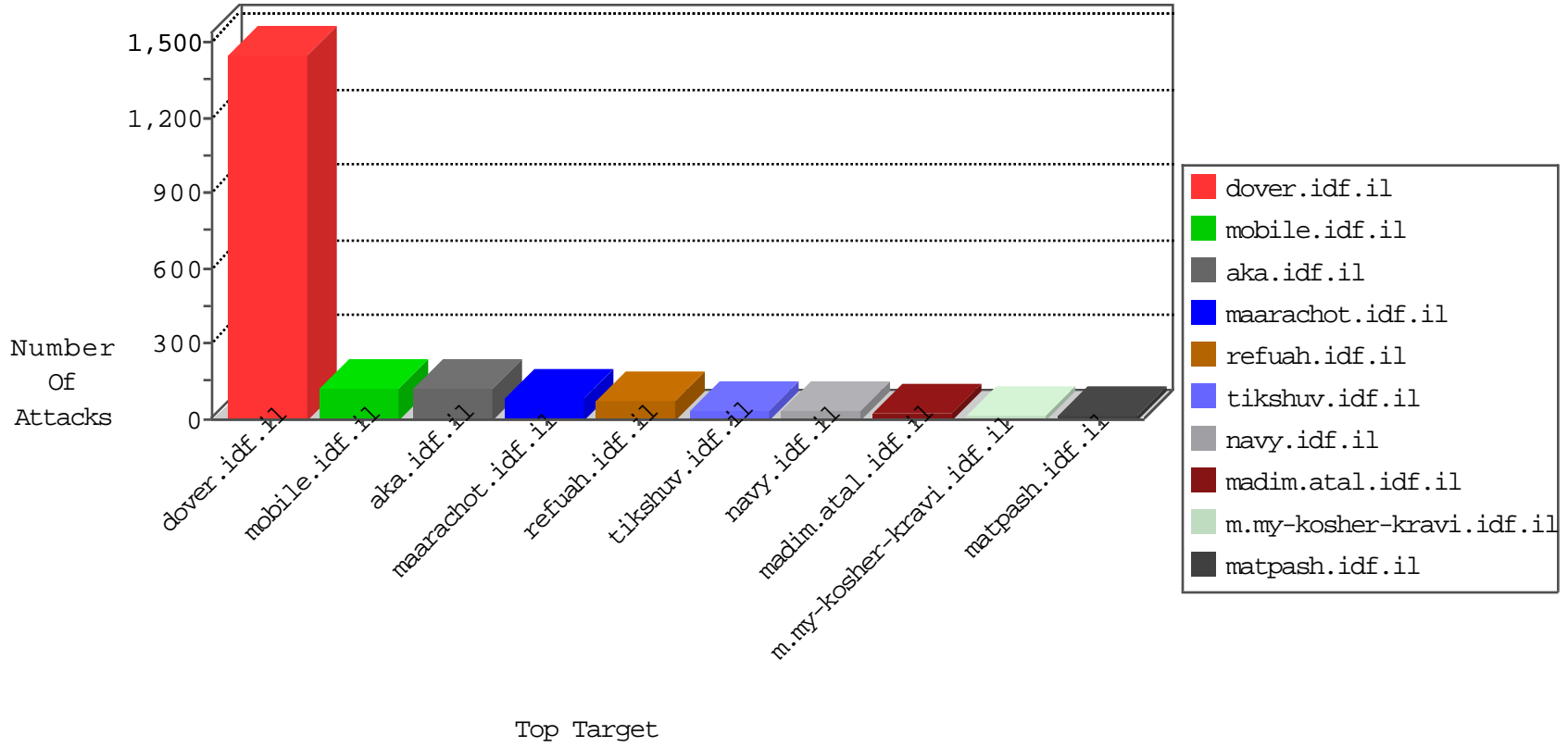


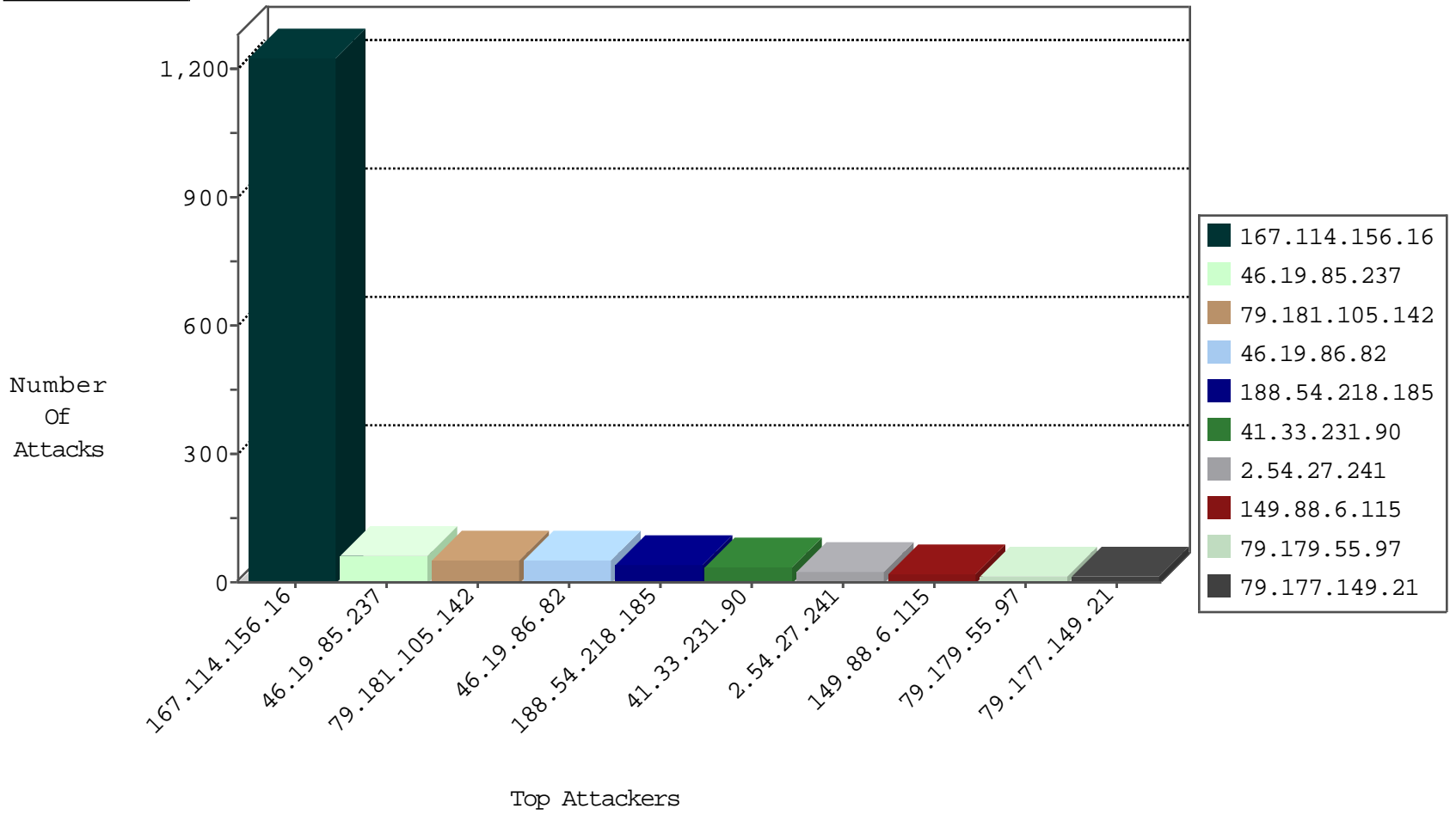
# IDF Under Attack Daily Report



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	3034
188.54.218.185	Saudi Arabia	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	2811
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4

01-01-2016-22:04:08 to 01-01-2016-23:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.54.218.185	Saudi Arabia	147.237.77.216	dover.idf.il	5141: HTTP: Sqlmap HTTP Request	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.237	147.237.76.42	Israel	refvuh.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	48
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
61.149.252.58	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
218.205.129.146	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
61.149.252.54	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
213.155.206.54	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN Potential SSH Scan	1
61.50.100.130	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
213.155.206.54	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
213.155.206.54	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
40.78.96.216	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
213.155.206.54	147.237.76.148	Russian Federation	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
36.110.44.178	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -f -sS	1
213.155.206.54	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
223.12.225.193	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.149.252.58	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -f -sS	1
218.205.129.146	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -f -sS	1
61.149.252.54	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -f -sS	1
213.155.206.54	147.237.77.176	Russian Federation	matpash.idf.il	ET SCAN Potential SSH Scan	1
61.50.100.130	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -f -sS	1
213.155.206.54	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN Potential SSH Scan	1
40.78.96.216	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
213.155.206.54	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN Potential SSH Scan	1
36.110.44.178	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
213.155.206.54	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
188.54.218.185	147.237.77.216	Saudi Arabia	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.181.105.142	Israel	147.237.77.243	mobile.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
46.19.86.82	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.54.27.241	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
149.88.6.115	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
79.177.149.21	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
79.179.55.97	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.64.79.140	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
176.12.136.0	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.181.119.96	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
149.50.77.38	United States	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
149.78.143.58	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.232	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.181.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.232	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.180.2.75	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.42.78	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
80.246.137.123	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.0	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.65.18	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.42.78	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	5
85.65.206.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
40.77.167.95	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.102.254.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
128.127.107.126	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
37.46.39.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
5.144.49.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.108.125.53	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
217.132.96.224	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
46.19.85.237	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
149.78.249.54	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
82.81.44.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.218	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.218	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.182.151.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	drop	SAM rule	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
185.3.147.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
81.7.17.171	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
37.26.146.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.121.68	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
79.179.14.39	Israel	147.237.77.216	dover.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
176.13.7.96	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	11
79.181.105.142	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	10
46.19.86.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.54.27.241	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.12.136.0	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
79.179.55.97	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.1.224	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
89.138.68.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.26.149.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.57.49.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.94.38.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.aspx/getauthuser	Block	2
109.253.197.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.14.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.7.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
105.105.190.63	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
79.181.135.73	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	2
185.3.144.49	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.218.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.64.8.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
141.212.122.160	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	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
5.144.49.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
82.81.44.211	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 5 in URL	Block	1
109.253.156.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.55.97	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1514	Block	1
185.65.135.227	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
149.210.158.71	Netherlands	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 149.210.158.71	Block	1
46.19.86.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.19.85.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.187.142.208	Czech Republic	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
188.138.1.218	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
149.210.158.71	Netherlands	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/arabic/pages/default.aspx	Block	1
46.19.86.233	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
41.131.97.114	Egypt	147.237.77.74	law.idf.il	PHP Attempt	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.228.42.78	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	1
46.19.85.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.218.200	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
166.78.134.156	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
46.121.198.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
41.131.97.114	Egypt	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
109.64.18.140	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1