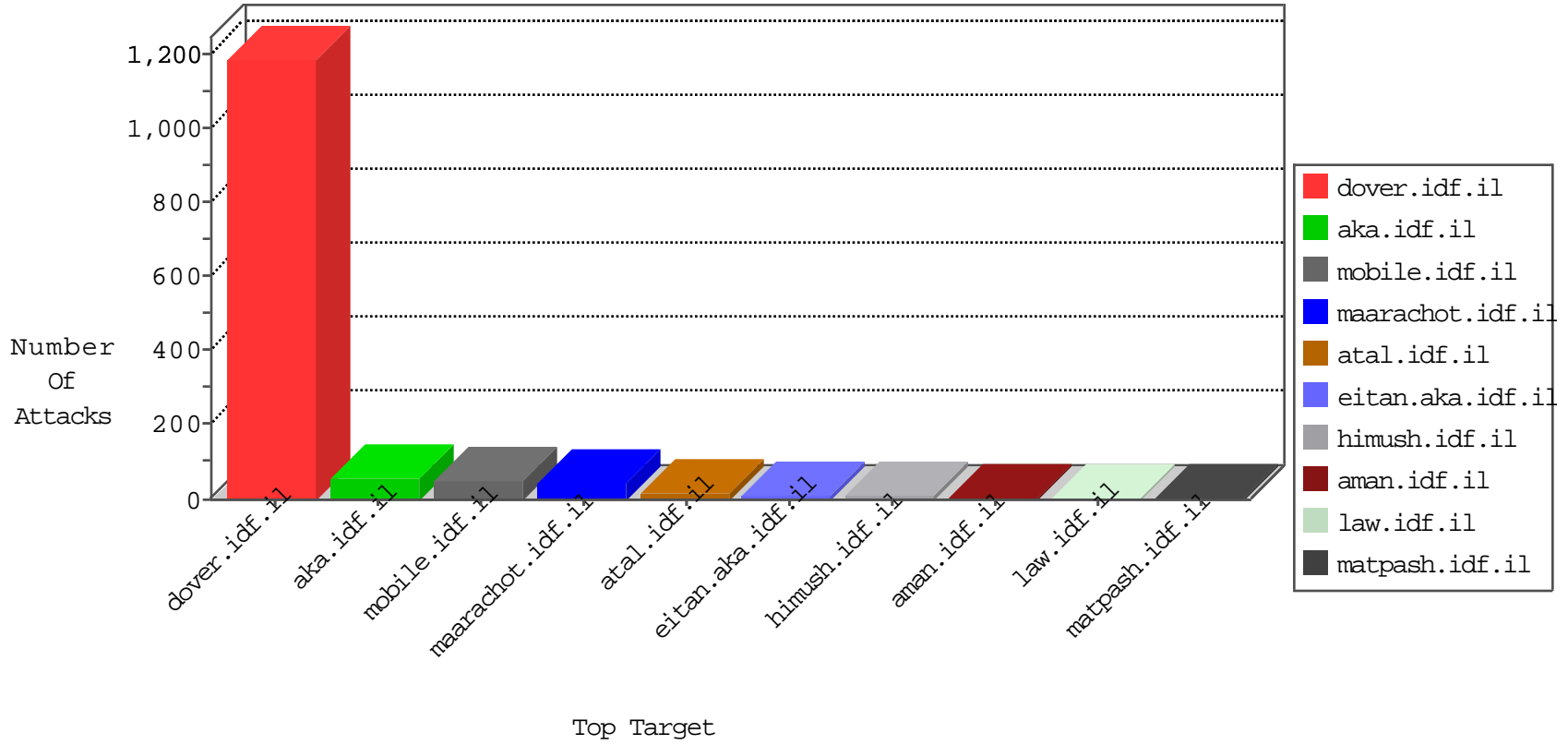


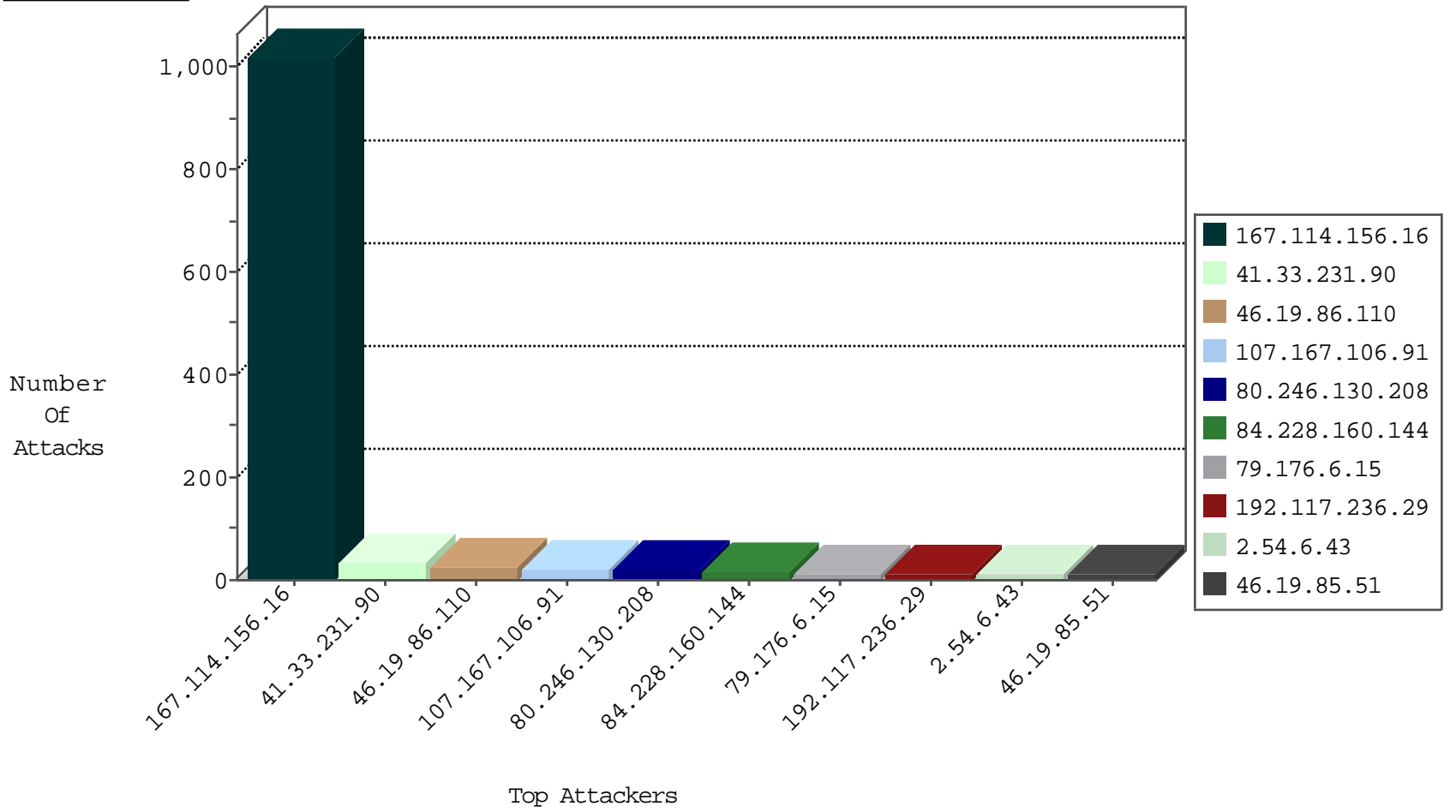
IDF Under Attack Daily Report



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	3077
204.42.253.2	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
180.97.106.37	China	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.5.224		147.237.72.166	aka.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
185.130.5.224		147.237.72.167	ishurim.aka.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
185.130.5.224		147.237.76.30	himush.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
185.130.5.224		147.237.76.42	refuah.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	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
80.246.130.208	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
46.151.52.195	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
12.139.41.189	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
192.198.216.130	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
121.183.175.167	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.77.227	Ukraine	e.hamaz.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
66.249.78.172	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
192.198.216.130	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
180.93.231.191	147.237.8.28	Vietnam	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
121.183.175.167	147.237.77.216	Korea, Republic of	dover.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.77.227	Ukraine	e.hamaz.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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
46.19.86.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
107.167.106.91	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
84.228.160.144	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
2.54.6.43	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.117.236.29	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	12
79.176.6.15	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.139.117	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.130.208	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.246.130.208	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.149.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
132.66.231.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.88.140.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
99.238.77.47	Canada	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.85.224	Israel	147.237.76.30	hinush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	4
46.121.94.141	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	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
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.60	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.52.189.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.45.254.226	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	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
149.78.22.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.130.84	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.85.236	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
94.230.86.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.12.149.63	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.102.254.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
31.210.188.107	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.90	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.83	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.88.140.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
213.57.57.113	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
2.52.189.29	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.116.140.60	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.172.232.207	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	7
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/error.htm	Block	2
87.68.34.91	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.183.63.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.12.149.63	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
85.64.97.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.176.6.15	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
109.253.136.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
86.47.80.146	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unknown Parameter sides*roll in www.aka.idf.il/giyus/kadatz/	None	1
188.143.232.16	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.16	Block	1
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method Accept-Language: in URL he-il,he	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.180.190.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
5.29.164.192	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
109.253.207.36	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
72.49.7.83	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
188.143.232.16	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.64.165	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/sip_storage/files/8/638.pds	Block	1
109.163.234.7	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.172	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
207.46.13.71	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
146.88.41.140	Thailand	147.237.72.166	aka.idf.il	Unknown Parameter siteid in www.aka.idf.il/sites/home/default.asp	None	1
89.139.231.138	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
72.49.7.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
195.154.194.111	France	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.65.27	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
109.186.170.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.139.117	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 112 cookies	Block	1
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
79.176.6.15	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
195.154.194.111	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.66.61	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/iraq/english/info07.asp	Block	1
109.201.154.207	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1
180.76.15.10	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9736-he/refuah.aspx	Block	1
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Malformed URL he-il,he;q=0.8,en-us;q=0.6,en;q=0.4	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
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	1