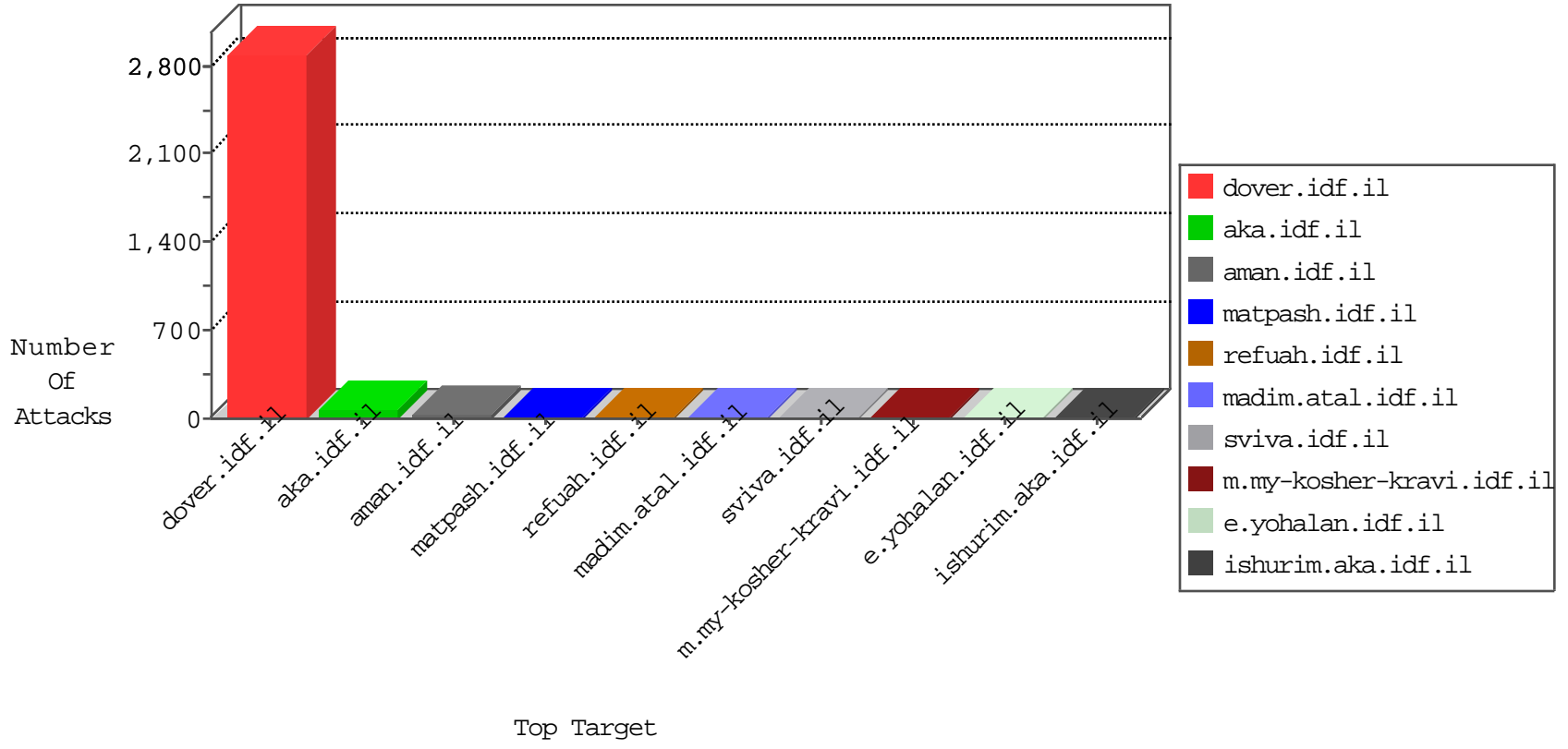


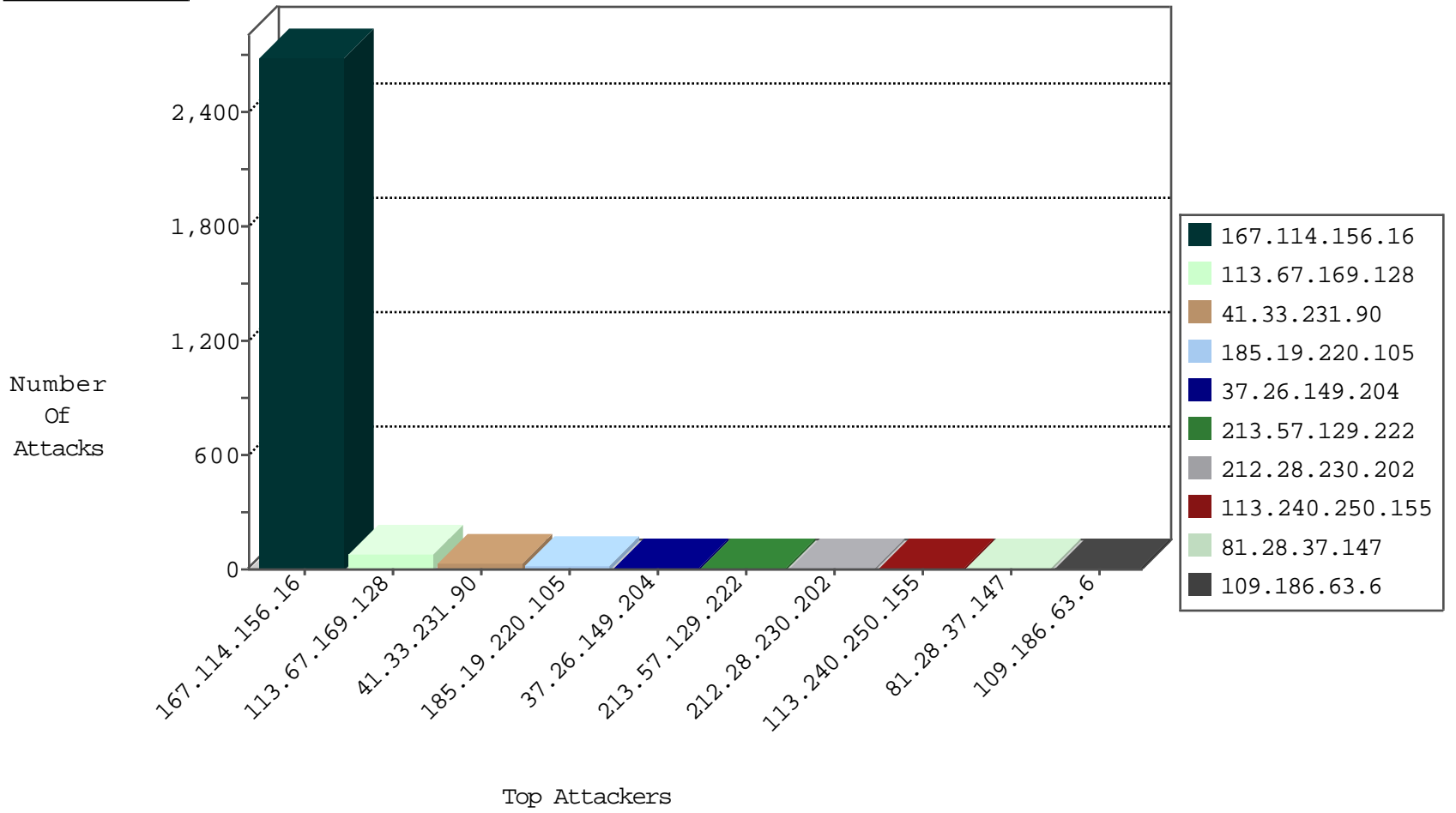
# IDF Under Attack Daily Report



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	3390
204.42.253.132	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
113.67.169.128	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
113.67.169.128	China	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	11
136.243.73.82	Germany	147.237.77.216	dover.idf.il	C1000106: 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
113.240.250.155	147.237.77.235	China	sviva.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
116.121.137.5	147.237.76.39	Korea, Republic of	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
113.240.250.155	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
62.212.73.196	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
62.212.73.196	147.237.76.148	Netherlands	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.0.34	Germany	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
204.151.10.118	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
204.151.10.118	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -f -sS	1
116.121.137.5	147.237.76.39	Korea, Republic of	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
97.105.43.174	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
62.212.73.196	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential SSH Scan	1
62.212.73.196	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
204.151.10.118	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 2048	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	32
185.19.220.105	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
185.19.220.105	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
109.186.63.6	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.28.230.202	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
93.172.42.112	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
213.57.130.102	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.142.96.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.184.111.116	Iran, Islamic Republic of	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
79.180.6.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.228.149.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.72.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.151.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.204	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.102.254.15	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.3.144.101	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.125.150.222	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.30.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.28.37.147	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
213.57.129.222	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
37.46.35.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.28.37.147	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
213.57.129.222	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
223.207.248.189	Thailand	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.137.166.102	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.129.222	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.148	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.64.1.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.142.68.110	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.26.146.216	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
141.212.121.192	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
87.69.63.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.149.204	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		alert	2
176.65.14.140	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.28.230.202	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
153.92.127.143	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
37.26.149.204	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	2
212.116.187.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.29.219.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.145	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.43.76.12	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
113.67.169.128	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
209.126.116.147	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.200	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.154.146.225	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
113.67.169.128	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 113.67.169.128	Block	25
176.13.8.9	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
79.183.96.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
113.67.169.128	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
176.13.4.68	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
109.66.207.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
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	2
216.218.206.68	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
197.37.37.121	Egypt	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/booklets.aspx	None	1
113.67.169.128	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/fck/	Block	1
37.238.28.6	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/qar/	Block	1
93.172.156.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.127.91.84	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	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
66.249.66.31	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
113.67.169.128	China	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
80.187.98.140	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
197.37.37.121	Egypt	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/portalmilium/templates/home.asp	Block	1
113.240.250.155	China	147.237.77.235	sviva.idf.il	Multiple Untraceable SSL Sessions from 113.240.250.155 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
93.173.226.34	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
77.237.154.221	Czech Republic	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	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
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
180.76.15.158	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
113.67.169.128	China	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 113.67.169.128	Block	1
5.28.147.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.111.41.234	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/1133-22461-he/dover.aspx.	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Unknown Parameter C@ID in www.aka.idf.il/giyus/general/	None	1
113.240.250.155	China	147.237.77.235	sviva.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.177.19.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resource/userfollowresource/create/	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
185.3.144.101	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 185.3.144.101	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17032-he/dover.aspx	Block	1
31.13.102.107	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/qar/	Block	1
85.140.7.61	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/idf/english/	Block	1
207.241.226.41	United States	147.237.76.30	himush.idf.il	Distributed PHP Attempt	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
114.98.232.198	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he/cogat.aspx/trackback/	Block	1
79.177.98.111	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.42.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.3.144.101	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
37.142.109.114	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1