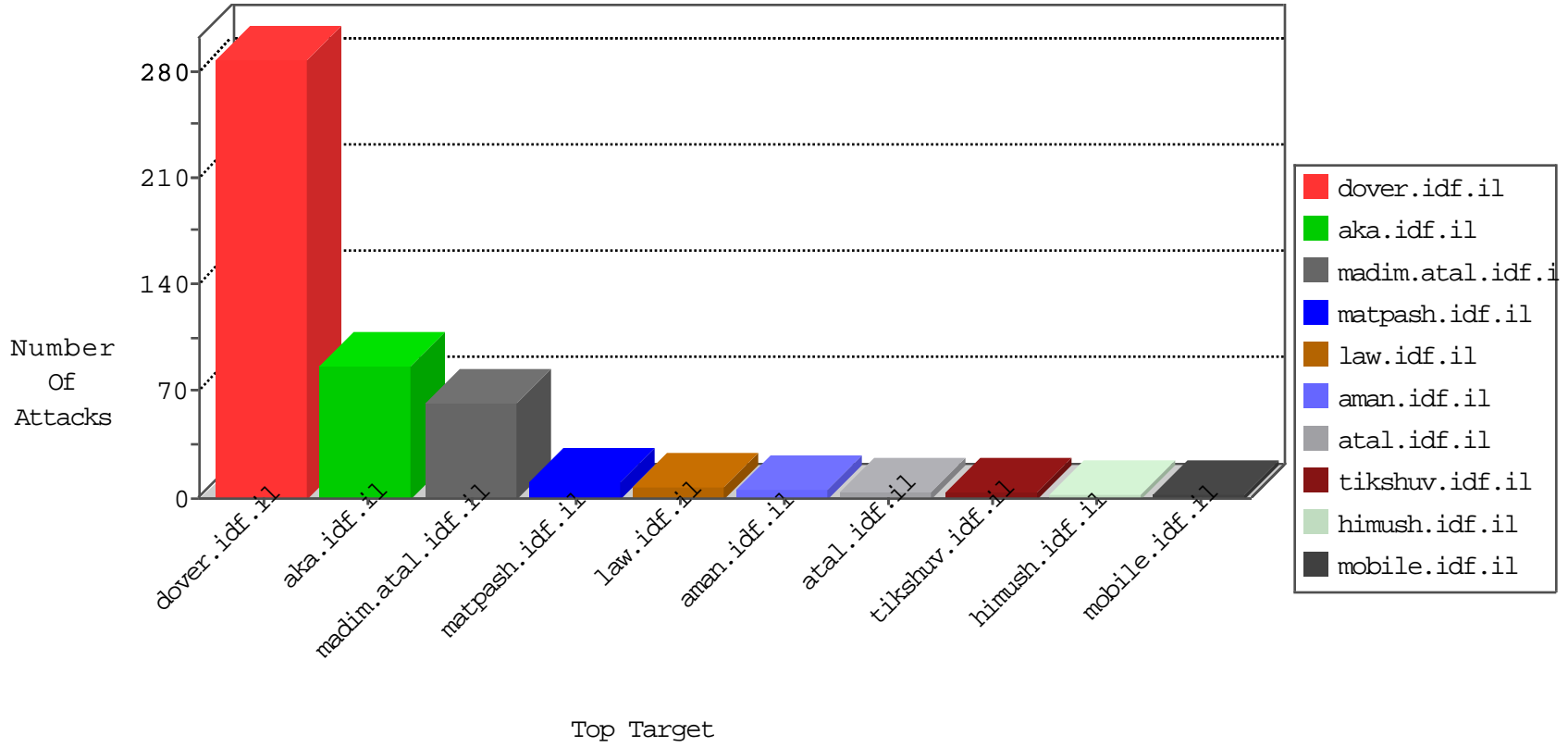


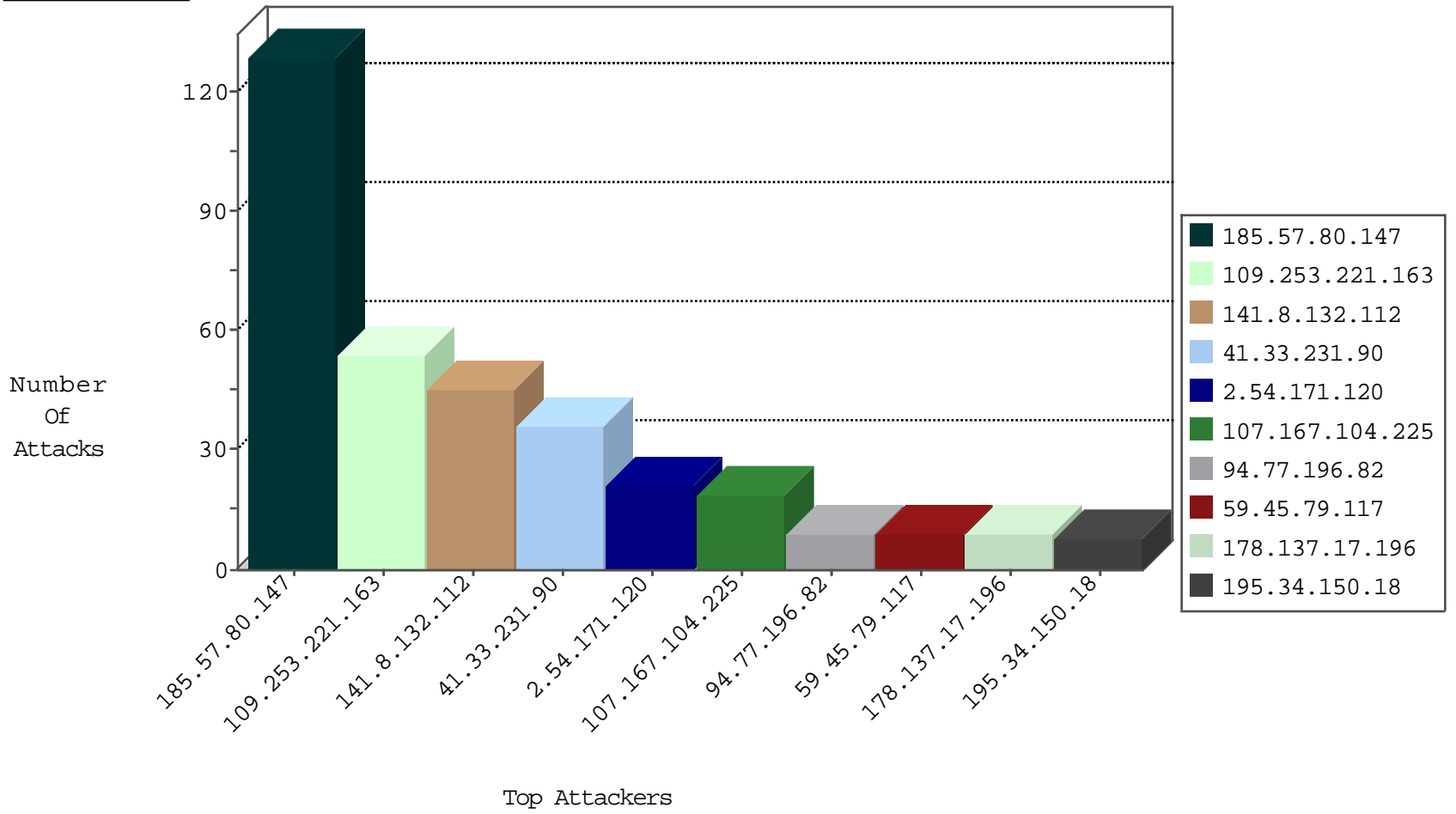
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
133.203.124.59	Japan	147.237.76.197	e.hinush.idf.il	Block_Udp_All_Nets	drop	1
159.122.252.41	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	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
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
148.163.122.135	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
123.126.113.80	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
59.45.79.117	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
198.54.90.200	147.237.72.166	United States	aka.idf.il	Tehila - Perl LWP with fake user agent	1
188.64.169.106	147.237.76.201	Russian Federation	e.atal.idf.il	ET SCAN Potential SSH Scan	1
148.163.122.135	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
107.167.104.225	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.54.171.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.116.29.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.171.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
2.54.171.120	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
82.145.211.57	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.171.120	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	4
109.253.198.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.194.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.158.152.201	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.132.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.13.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.41.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.139.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.95.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.171.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
108.167.133.30	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	2
85.65.44.52	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.120.126.35		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
138.134.192.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.54.171.120	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.185.4.108	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
85.64.165.81	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.115	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.48	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
23.242.161.57	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
213.57.241.57	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
70.39.186.218	Satellite Provider	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
184.105.139.79	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
45.79.168.168		147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
115.230.124.164	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
74.82.47.48	United States	147.237.76.30	hinush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.251.203.200	Greece	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
176.13.3.23	Israel	147.237.72.166	aka.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
216.218.206.70	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
70.39.186.222	Satellite Provider	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
184.105.139.116	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 185.57.80.147	Block	128
109.253.221.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
178.137.17.196	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	9
109.253.209.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
89.139.232.217	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 89.139.232.217	Block	3
199.30.24.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.241	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.16.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.139.232.217	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
17.138.58.91	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	2
157.55.2.154	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.2.156	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
89.139.232.217	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/ajax/updatestatus.php	Block	1
46.117.234.33	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
173.32.146.39	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
211.34.109.207	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.31.32.28		147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
157.55.39.198	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
109.253.147.182	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$82 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
59.152.202.68	Hong Kong	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
69.58.178.59	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/shared/usercontrols/headerupper/	Block	1
2.54.8.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$96 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
167.114.156.198	Canada	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.64.234	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
203.133.168.203	Korea, Republic of	147.237.76.200	eitan.aka.idf.il	Unknown Parameter l in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
148.251.21.227	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jeninkilled/stn	Block	1
185.57.80.147	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/3201843258186756357.aspx	Block	1
167.114.156.198	Canada	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/shared/usercontrols/headerupper/	Block	1
109.253.213.32	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$2 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
211.31.161.118	Australia	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
184.105.247.195	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
46.117.85.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cblQuestion\$120 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
195.154.226.90	France	147.237.77.74	law.idf.il	Illegal HTTP Version HTTP/	Block	1
173.32.146.39	Canada	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
211.31.161.118	Australia	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
66.249.75.20	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
185.31.32.28		147.237.77.74	law.idf.il	PHP Attempt	Block	1