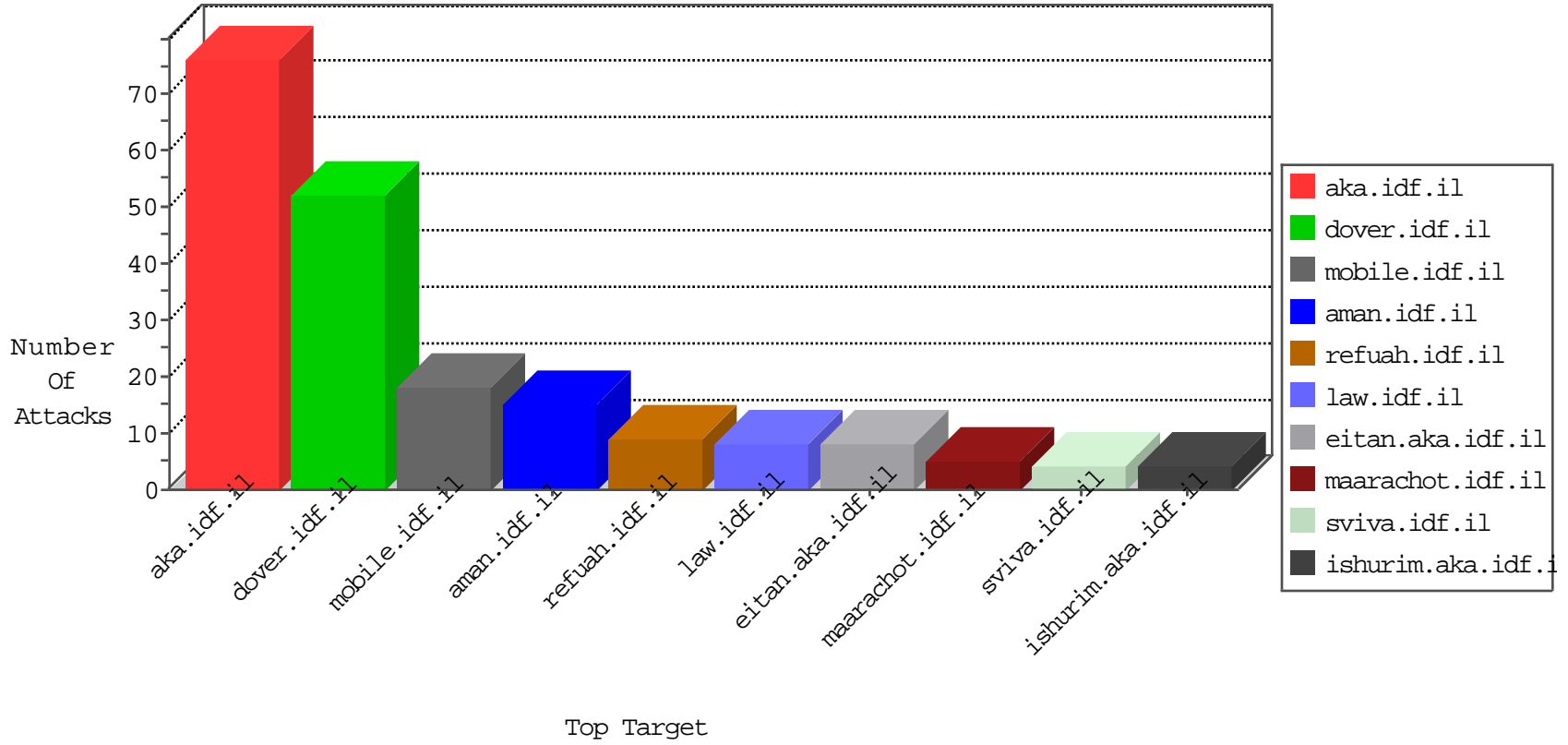


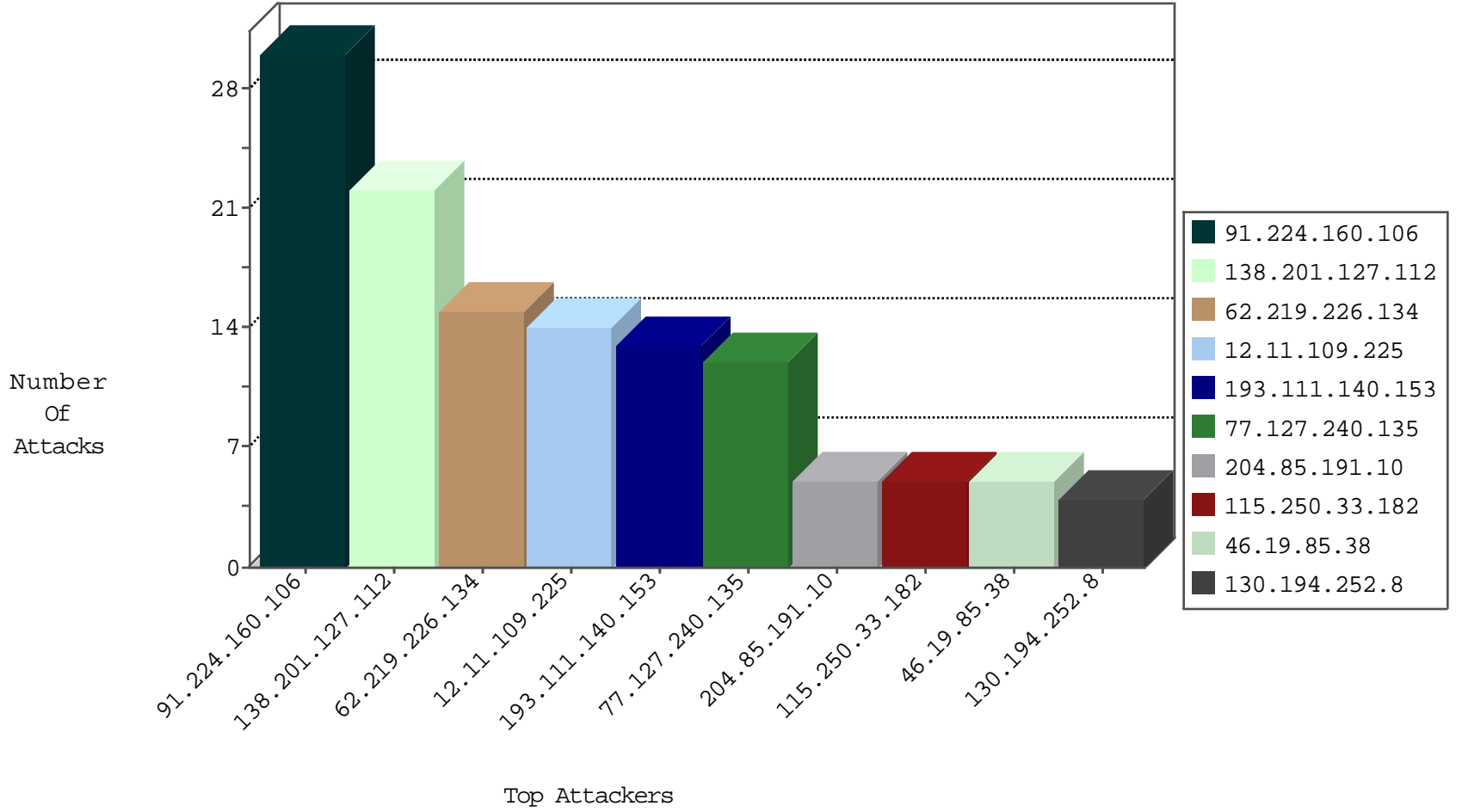
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.111	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.34	Germany	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
165.242.90.128	Japan	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
141.212.113.178	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.84	Czech Republic	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
177.75.200.167	Brazil	147.237.77.243	mobile.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.221	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.12	Ireland	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
138.201.127.112	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	22
193.111.140.153	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	9
193.111.140.153	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	4

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.224.160.106	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential SSH Scan	2
5.255.90.133	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
193.23.181.171	147.237.0.33	Ukraine	idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential SSH Scan	1
182.52.236.242	147.237.77.170	Thailand	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
91.224.160.106	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
163.172.129.15	147.237.77.170	United Kingdom	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.160.106	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
212.227.55.94	147.237.77.235	Germany	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.73	147.237.76.30	Ukraine	himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
182.52.236.242	147.237.77.170	Thailand	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
91.224.160.106	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
182.52.236.242	147.237.77.170	Thailand	maarachot.idf.il	ET SCAN NMAP -f -sS	1
91.224.160.106	147.237.76.148	Netherlands	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
103.207.39.82	147.237.0.34	Vietnam	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1
66.249.73.171	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
193.201.225.73	147.237.76.42	Ukraine	refuah.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
62.219.226.134	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
12.11.109.225	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
115.250.33.182	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.38	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
77.127.240.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.16.179	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
199.30.24.137	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
77.127.240.135	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.127.240.135	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
213.151.42.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
77.127.240.135	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
141.226.162.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
180.97.106.161	China	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
106.186.113.169	Japan	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
59.165.238.74	India	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
192.168.173.102		147.237.77.216	dover.idf.il	drop		drop	1
162.216.46.151	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
24.183.99.4	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.161	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
176.13.248.193	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
46.19.85.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
180.97.106.161	China	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
141.212.122.120	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.16	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.37	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
84.108.226.42	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.97.106.161	China	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
141.212.122.121	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.29.75.90	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.37	China	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1
84.108.226.42	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.97.106.162	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.72.44.245	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/chinuch/home/default.asp	Block	2
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	2
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
85.130.185.243	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
109.253.143.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/gyus/forum/asp/showforum.asp	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
157.55.39.19	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1
66.249.64.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/gyus/forum/asp/showforum.asp	Block	1
46.19.86.134	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1412-he/atal.aspx	Block	1
157.55.39.196	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/smalim/showbig.aspx	None	1
66.249.64.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/piwik.php	Block	1
64.30.76.149	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1