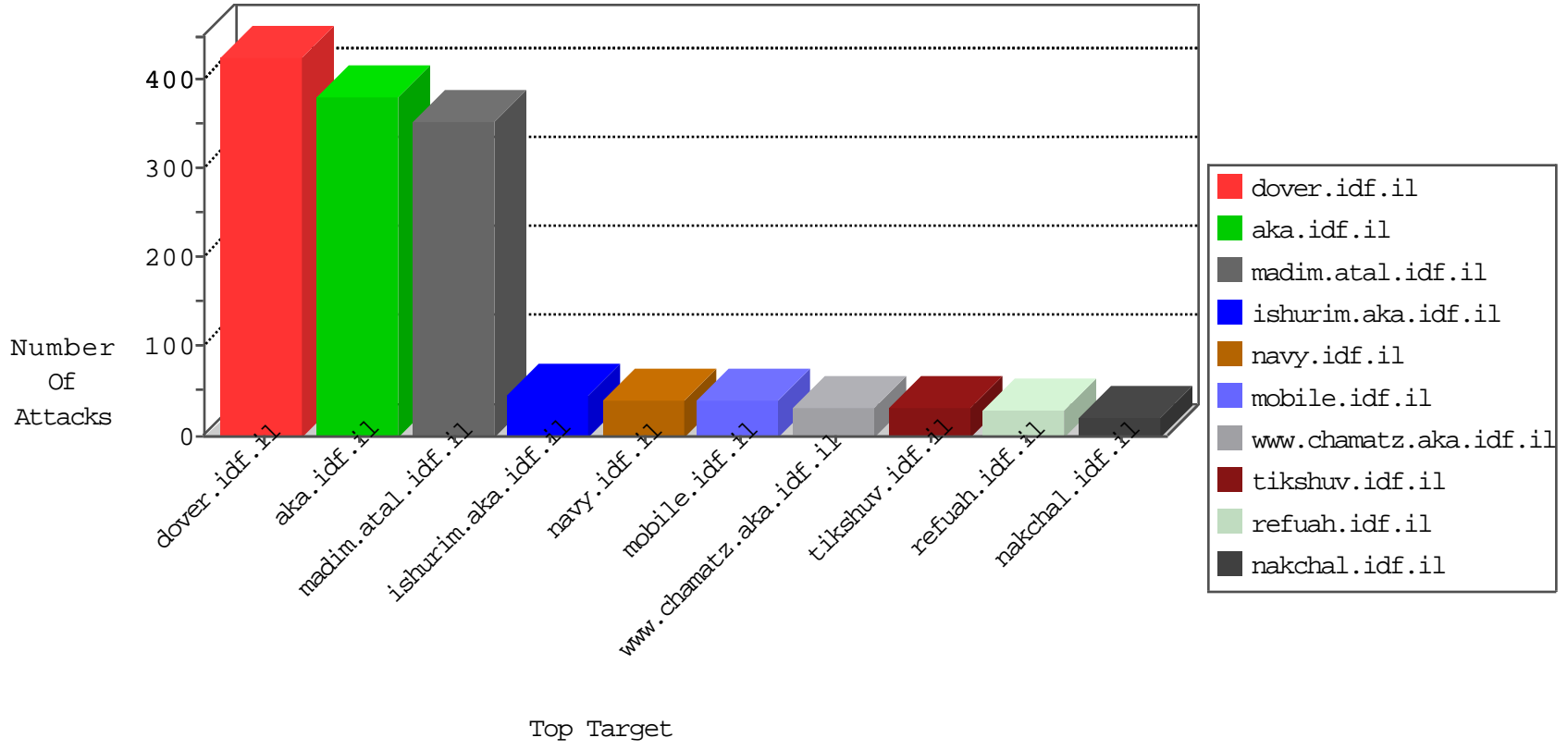


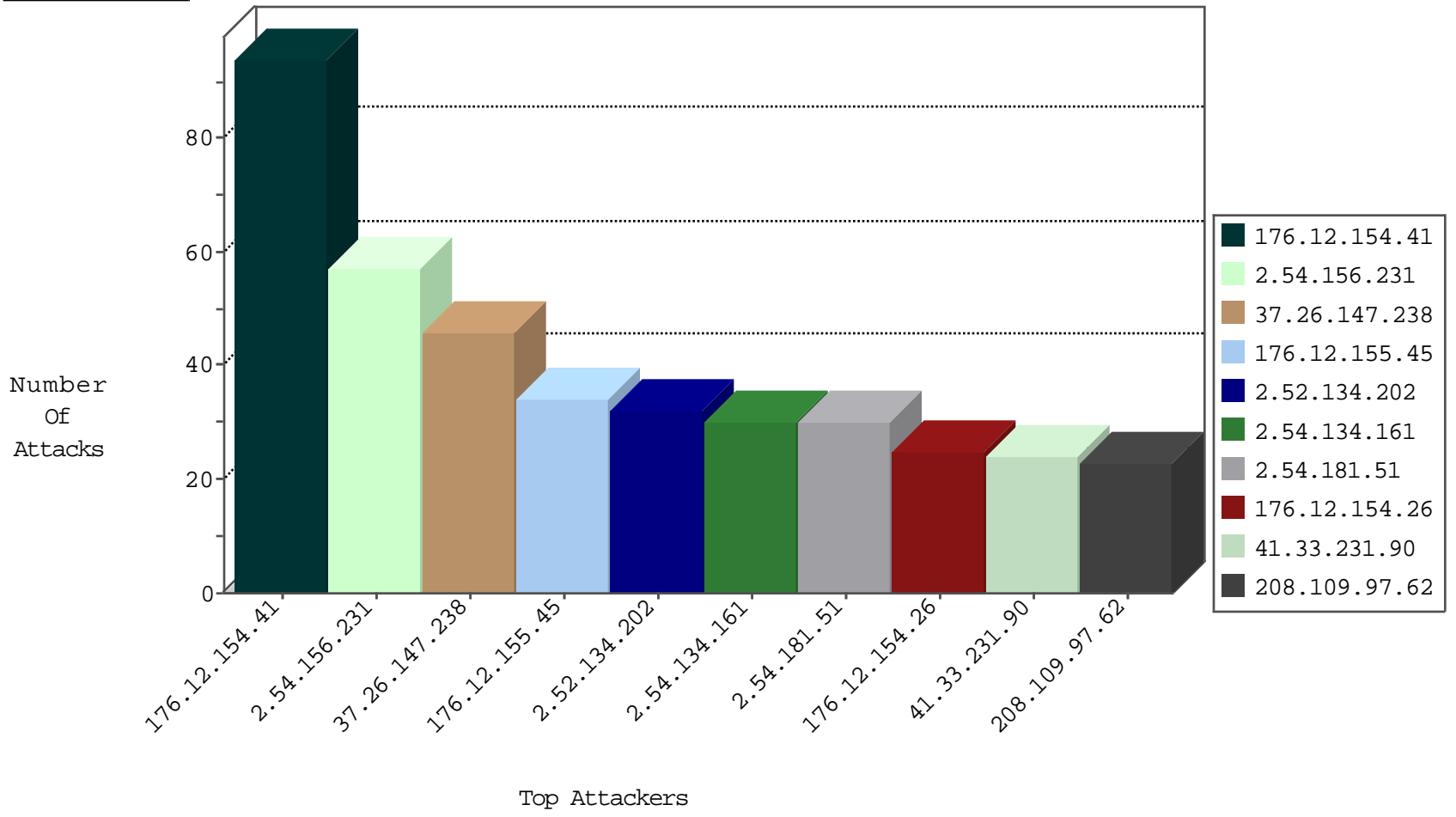
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	30
208.109.97.62	United States	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	23
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	10
124.232.137.57	China	147.237.76.148	ggcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
115.230.124.164	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
115.239.228.10	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
159.220.78.115	India	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.220.78.116	India	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
159.220.78.113	India	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.130.5.201		147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
159.220.78.114	India	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.207.27	United Kingdom	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
------------------	----------------	------------------	------	-----------	-------

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	24
207.241.229.192	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	22
2.54.156.231	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	20
2.54.181.51	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
212.76.127.219	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
31.168.52.118	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.19.85.7	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
2.54.156.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
176.12.155.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.94.36.69	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
213.8.204.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.76.127.10	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
80.246.130.163	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.15	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
77.125.151.131	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
84.95.2.160	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.156.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
46.19.85.38	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
2.54.156.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.54.156.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.246.130.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
89.138.27.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.111.1.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.152.25	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.12.154.133	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.165.173	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.149.163	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.160.191.56	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
62.0.207.1	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
79.181.230.49	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.160.191.56	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.180.124.112	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
106.186.19.160	Japan	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.60	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.226.48.84	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.183.106.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.131.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.51	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.199.121.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.165	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.7	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.253.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.199.121.158	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
31.210.187.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.154.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
37.26.147.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
176.12.155.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
2.54.134.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
2.52.134.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
176.12.154.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
185.32.179.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
159.149.217.50	Italy	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 159.149.217.50	Block	17
46.121.37.45	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
80.246.138.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
80.246.137.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
176.12.154.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
84.108.172.56	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
37.26.147.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
46.19.86.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
95.86.106.49	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 95.86.106.49	Block	7
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	6
37.26.149.175	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	5
62.219.127.53	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	3
176.12.155.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.154.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.203.226.21	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.86.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.12.155.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.219.127.53	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 62.219.127.53	Block	2
80.246.137.169	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.65.169.142	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
87.69.69.144	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
2.54.146.80	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
79.180.117.124	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https://www.aman.idf.il/	Block	1
217.69.133.220	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter docId&pageNum in aka.idf.il/tizmoret/faq/default.asp	None	1
104.131.147.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
5.102.202.125	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
176.12.155.229	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
77.125.140.97	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https://www.aman.idf.il/	Block	1
176.12.154.26	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	1
141.212.122.177	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
65.19.167.131	United States	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
89.138.180.200	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$ct100\$txtSearch in www.aka.idf.il/main/giyus/pniotfindanswer.aspx	None	1
40.77.167.63	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/894-7860-he	Block	1
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
2.54.187.146	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
166.63.123.145	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
54.167.183.116	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/589-he/patzar.aspx=	Block	1
105.28.98.212	Mauritius	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
81.218.56.171	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 81.218.56.171	Block	1
31.168.52.118	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1