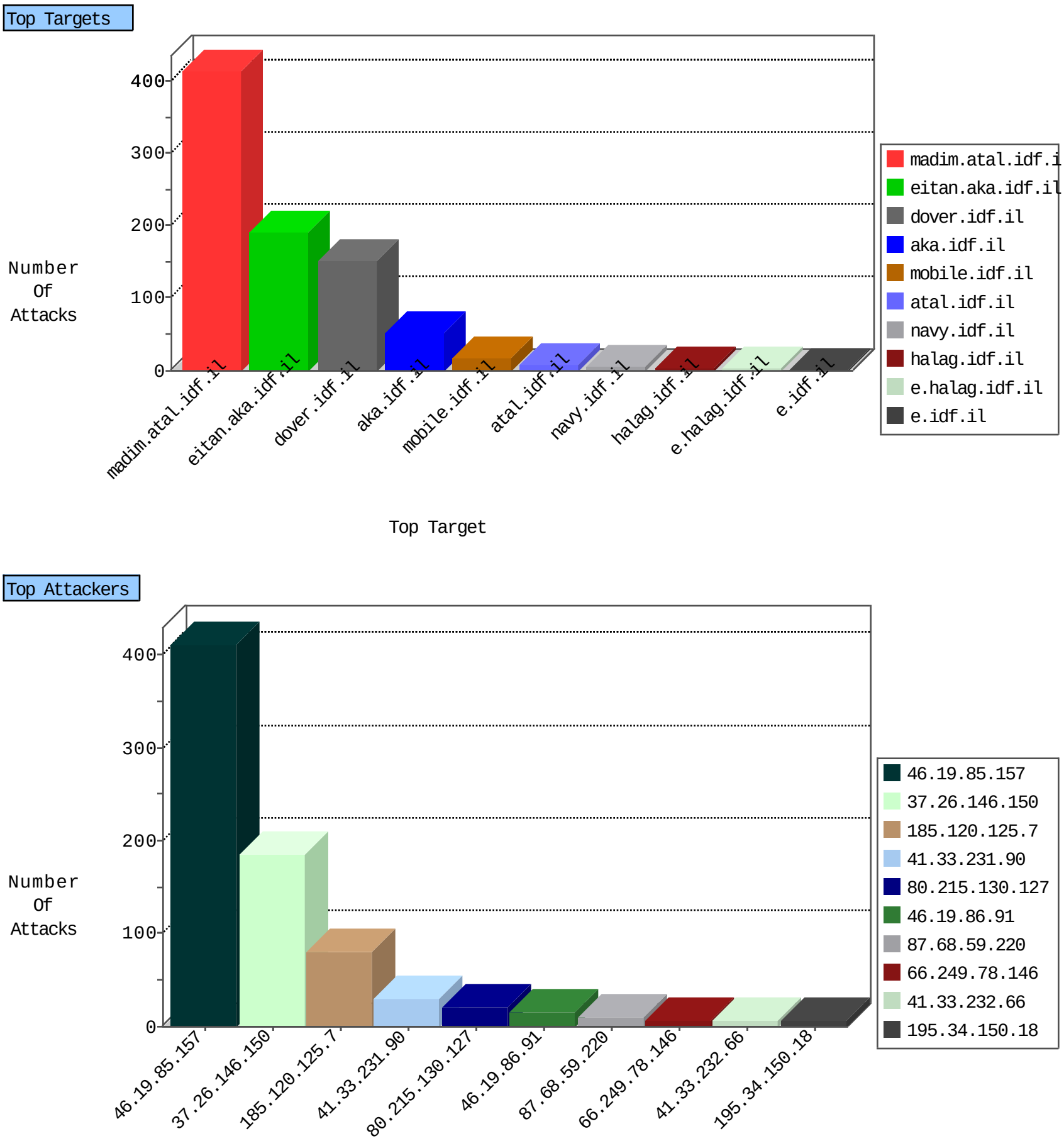
02-02-2016-02:04:05 to 02-02-2016-03:04:05

IDF Under Attack Daily Report



02-02-2016-02:04:05 to 02-02-2016-03:04:05

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	2
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
178.239.62.139	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1

02-02-2016-02:04:05 to 02-02-2016-03:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.190.10	France	147.237.77.216	dover.idf.il	19791: HTTP: WordPress N-Media PHP File Upload	Block	1

02-02-2016-02:04:05 to 02-02-2016-03:04:05

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	3
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
124.43.21.107	147.237.76.202	Sri Lanka	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
124.43.21.107	147.237.76.202	Sri Lanka	e.halag.idf.il	ET SCAN NMAP -f -sS	1
109.235.254.181	147.237.77.234	Turkey	halag.idf.il	ET SCAN NMAP -sS window 1024	1
124.43.21.107	147.237.76.202	Sri Lanka	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
121.201.27.61	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1

02-02-2016-02:04:05 to 02-02-2016-03:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.146.150	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	186
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	27
80.215.130.127	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
46.19.86.91	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.68.59.220	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.85.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.216	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.177.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
87.68.59.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
198.182.56.5	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
66.249.64.139	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.159	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.147	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.151	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
50.87.113.190	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
174.56.74.169	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.148	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.152	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
65.78.23.68	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
178.162.199.95	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.150	United States	147.237.0.33	idf.il	drop		drop	1
69.167.168.241	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.19.85.221	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.152	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
65.78.23.68	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.151	United States	147.237.0.33	idf.il	drop		drop	1
45.79.168.168		147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.158	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
136.243.67.234	Germany	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.19.85.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.255.253.38	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.151	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

02-02-2016-02:04:05 to 02-02-2016-03:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	262
46.19.85.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	150
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
46.19.86.91	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
62.210.190.10	France	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
176.12.154.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
40.77.167.32	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
212.1.210.166	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wp/wp-admin/	Block	1
94.1.179.43	United Kingdom	147.237.76.86	navy.idf.il	NULL Character in Method Â,[[#0]][[#0]][[#0]][[#19]]Ã±[Ã‰Ã™ Ã?`Â¿ÂªÂ?Â¾ÂŸHfÃ”6[[#16]][[#7]]Â?Â¹,ÃƒÃ‚Ã—ÃµSSÂ‚6Ã€[[#30]]Â©Â' [[#25]]ÂªÂ±VcKÂ¼Ã¼Â•Ã‹[[#16]]Â-Â½-$Lur8Ã¹Â²!Ã'ÃœÂƒ:[[#1]]Ã„ %Â?[[#12]]Ã§[[#28]]Ã?qÃ«Â°Â?[[#29]]Â“Â?ÃŠÃ½Ã°[[#2]]Ãœ[[#25]]	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
62.210.190.10	France	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
184.106.177.53	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/test/wp-admin/	Block	1
94.1.179.43	United Kingdom	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/ishurim/cityofficers/	None	1
40.77.167.35	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim/fund/Ã£â€"Ã¢â‚¬Ëœâ€" Ã¢â‚¬Â?Ã£â€"Ã¢Â§Ã£â€"Ã¥Â¾Ã£â€"Ã¢â‚¬Â?	Block	1
157.55.39.55	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/sip_storage/files/5/2495.jpg	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
62.210.190.10	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.210.190.10	Block	1
195.114.18.165	France	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wp-admin/	Block	1
94.1.179.43	United Kingdom	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Header Name	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
157.55.39.58	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/sip_storage/files/4/2534.jpg	Block	1
74.208.16.10	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/old/wp-admin/	Block	1
198.20.69.74	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
94.1.179.43	United Kingdom	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method Â,[[#0]][[#0]][[#0]][[#19]]Ã±[Ã‰Ã™ Ã?`Â¿ÂªÂ?Â¾ÂŸHfÃ”6[[#16]][[#7]]Â?Â¹,ÃƒÃ‚Ã—ÃµSSÂ‚6Ã€[[#30]]Â©Â' [[#25]]ÂªÂ±VcKÂ¼Ã¼Â•Ã‹[[#16]]Â-Â½-$Lur8Ã¹Â²!Ã'ÃœÂƒ:[[#1]]Ã„ %Â?[[#12]]Ã§[[#28]]Ã?qÃ«Â°Â?[[#29]]Â“Â?ÃŠÃ½Ã°[[#2]]Ãœ[[#25]]	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/haredim/general.aspx	None	1
157.55.39.142	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1116-he/Ã£Æ'Ã¦â€™Ã£Â¢Ã¢â€š Â¬Ã¢â‚¬Â?Ã£Æ'Ã¢â‚¬Å¡Ã£â€šÃ¢Â¦Ã£Æ'Ã¦â€™Ã£Â¢Ã¢â€šÂ¬Ã¢â‚¬Â?Ã£Æ' Ã¢Â¢Ã£Â¢Ã¢â‚¬Å¡Ã¢Â¬Ã£â€šÃ¢Â?	Block	1
87.68.59.220	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
62.210.190.10	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-admin/admin-ajax.php	Block	1
24.189.82.242	United States	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
202.218.6.8	Japan	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wordpress/wp-admin/	Block	1
94.1.179.43	United Kingdom	147.237.76.86	navy.idf.il	Illegal HTTP Version	Block	1
93.129.97.45	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1

02-02-2016-02:04:05 to 02-02-2016-03:04:05