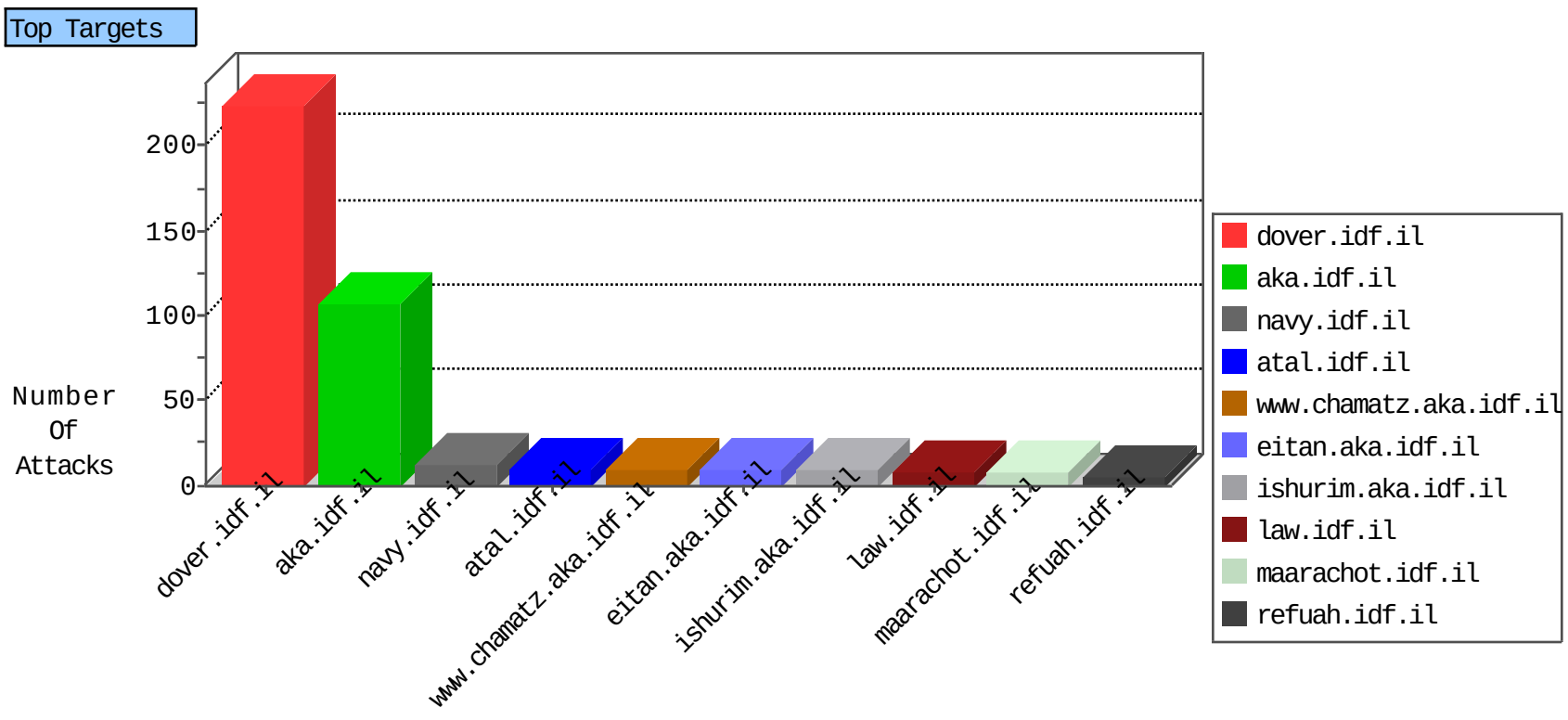
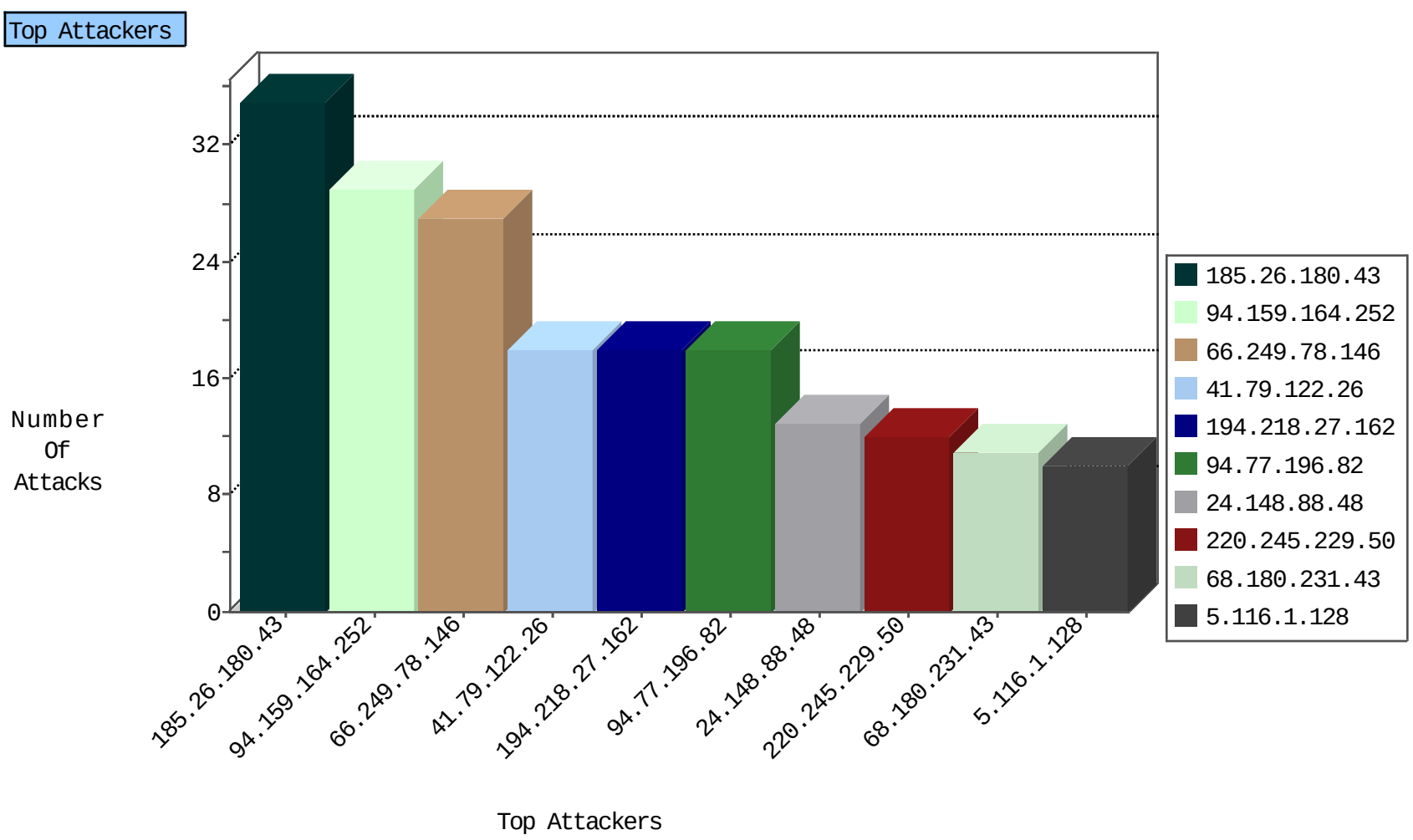
04-20-2016-06:04:01 to 04-20-2016-07:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-20-2016-06:04:01 to 04-20-2016-07:04:01

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	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	3
185.103.252.141	Russian Federation	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
73.141.192.115	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

04-20-2016-06:04:01 to 04-20-2016-07:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-20-2016-06:04:01 to 04-20-2016-07:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
89.234.68.82	147.237.72.167	Ireland	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	7
86.47.80.146	147.237.77.216	Ireland	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
85.131.208.140	147.237.0.200	Germany	m4u.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.8.27	Netherlands	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.205.69	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
40.69.45.42	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
183.60.48.25	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
36.72.228.72	147.237.76.176	Indonesia	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
151.11.201.3	147.237.77.74	Italy	law.idf.il	ET SCAN NMAP -sS window 4096	1
36.72.228.72	147.237.76.176	Indonesia	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
113.240.250.154	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
104.130.70.221	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
187.185.81.117	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.218.205.69	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
40.69.45.42	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
183.60.48.25	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
40.69.45.42	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
173.65.154.27	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
36.72.228.72	147.237.76.176	Indonesia	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
151.11.201.3	147.237.77.74	Italy	law.idf.il	ET SCAN NMAP -sS window 3072	1
107.158.255.194	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1

04-20-2016-06:04:01 to 04-20-2016-07:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
94.159.164.252	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
185.26.180.43	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
41.79.122.26	N/A	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
24.148.88.48	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
185.26.180.43	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
37.26.146.163	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
79.181.215.138	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
220.245.229.50	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.116.1.128	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.146.139	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.55.38.211	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
220.245.229.50	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
54.236.1.77	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.116.1.128	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
62.128.48.84	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
65.55.210.126	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.236.1.67	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
149.202.98.160	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.98.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.164.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.98.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
46.19.86.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.254	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
64.246.161.30	United States	147.237.77.233	atal.idf.il	Header Rejection	header rejection pattern found in request	monitor	3
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.98.182	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	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
176.13.13.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
68.180.229.154	United States	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
68.180.229.170	United States	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.250.0.222	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
96.226.203.155	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
212.199.182.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
68.180.229.154	United States	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	2
2.53.150.226	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.79.120.18	N/A	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
68.180.229.170	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	2

04-20-2016-06:04:01 to 04-20-2016-07:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.114.102	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	2
89.234.68.82	Ireland	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
86.47.80.146	Ireland	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.199	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/yohalan/main0926.html	Block	1
104.128.144.131	Canada	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
41.239.143.16	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
87.71.61.25	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
130.185.155.10	Sweden	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
80.246.133.27	Israel	147.237.77.176	matpash.idf.il	Parameter Type Violation toDate in www.cogat.idf.il/901-he/cogat.aspx	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8762-he/refuah.aspx	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1927-en/cogat.aspx gaza semanales	Block	1
38.111.147.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
130.185.155.10	Sweden	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/wp-login.php	Block	1
84.95.85.112	Israel	147.237.72.166	aka.idf.il	Unknown Parameter y in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9740-he/refuah.aspx	Block	1
40.77.167.44	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
178.49.154.149	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/894-he/chinuch.aspx	Block	1
86.47.80.146	Ireland	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 86.47.80.146 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.75.118	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/	Block	1
104.128.144.131	Canada	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to 147.237.76.147/	Block	1
74.111.42.147	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	1
40.77.167.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1

04-20-2016-06:04:01 to 04-20-2016-07:04:01