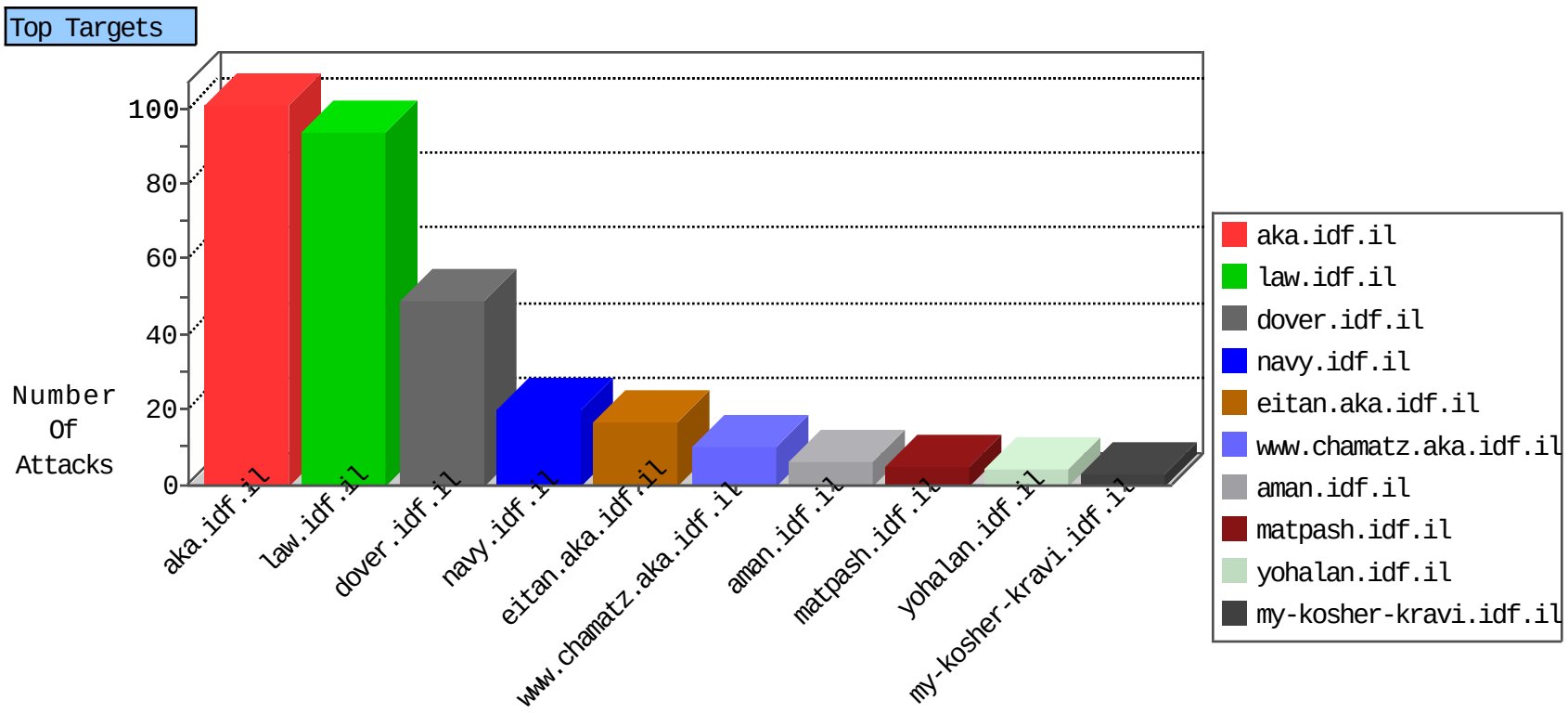
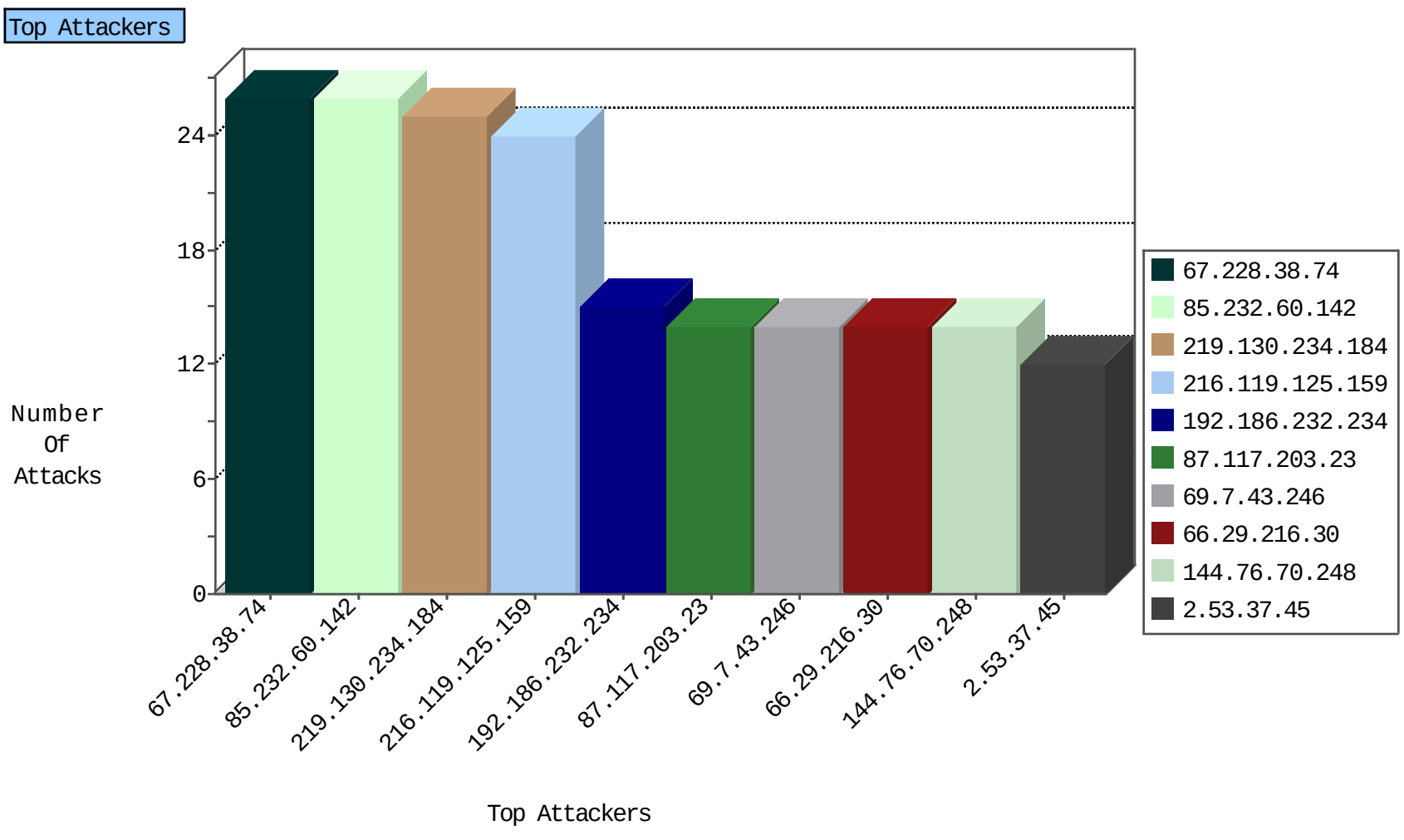
09-01-2016-03:04:00 to 09-01-2016-04:04:00

IDF Under Attack
Daily Report





09-01-2016-03:04:00 to 09-01-2016-04:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
168.235.197.59	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
120.76.24.17	China	147.237.8.27	e.madim.atal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

09-01-2016-03:04:00 to 09-01-2016-04:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.232.60.142	United Kingdom	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
67.228.38.74	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
87.117.203.23	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
69.7.43.246	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
144.76.70.248	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.125.159	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
66.29.216.30	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
85.232.60.142	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
67.228.38.74	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
69.30.198.178	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-01-2016-03:04:00 to 09-01-2016-04:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
216.119.125.159	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	18
85.232.60.142	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	14
67.228.38.74	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
132.72.138.1	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	8
87.117.203.23	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	8
69.7.43.246	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
66.29.216.30	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
144.76.70.248	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	8
137.117.80.189	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	4
24.250.165.200	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
58.218.204.245	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
46.227.67.172	147.237.0.35	Sweden	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
222.254.34.165	147.237.76.34	Vietnam	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
24.250.165.200	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
201.238.202.219	147.237.0.15	Chile	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
24.250.165.200	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
24.250.165.200	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.227.67.172	147.237.0.17	Sweden	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
24.250.165.200	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1

09-01-2016-03:04:00 to 09-01-2016-04:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
2.53.37.45	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
89.139.151.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.78	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
87.106.184.160	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
61.220.26.201	Taiwan	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
192.186.232.234	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
199.30.16.187	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.186.232.234	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
66.249.76.106	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.186.232.234	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
197.39.140.193	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.28.111	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
192.186.232.234	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
192.186.232.234	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
78.144.77.221	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
185.69.4.235	Iraq	147.237.76.34	yohalan.idf.il	drop		drop	2
64.246.178.34	United States	147.237.76.86	navy.idf.il	Header Rejection	header rejection pattern found in request	monitor	2
78.144.77.221	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	2
78.144.77.221	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
107.167.112.188	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
141.212.122.32	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
222.254.34.165	Vietnam	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
62.138.2.83	Germany	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.13.249.197	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.47	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
120.132.95.94	China	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.37	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
222.254.34.165	Vietnam	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
89.139.151.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
181.104.103.176	Argentina	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
169.229.3.91	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
137.226.113.7	Germany	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
212.179.20.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.233.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.38	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
222.254.34.165	Vietnam	147.237.76.34	yohalan.idf.il	drop		drop	1
185.20.5.157	United Kingdom	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
169.229.3.91	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
137.226.113.7	Germany	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
212.179.20.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
62.138.2.83	Germany	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
176.13.233.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.44	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
222.254.34.165	Vietnam	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.222.192.163	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
185.20.5.157	United Kingdom	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	1

09-01-2016-03:04:00 to 09-01-2016-04:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
219.130.234.184	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 219.130.234.184	Block	18
219.130.234.184	China	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
66.249.76.35	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.35	Block	2
219.74.104.33	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.71	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
213.151.62.217	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/may/bethlehem2.stm" target="_blank	Block	1
219.130.234.184	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
203.127.96.216	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
216.244.66.231	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.76.100	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list20041220a.htm	Block	1
220.255.145.120	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.64	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/about_our_courses.asp	Block	1
66.249.76.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/assetlinks.json	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
61.8.202.103	Singapore	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
212.199.144.158	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
132.72.138.1	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.80	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/1072-	Block	1
212.199.144.158	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	1

09-01-2016-03:04:00 to 09-01-2016-04:04:00