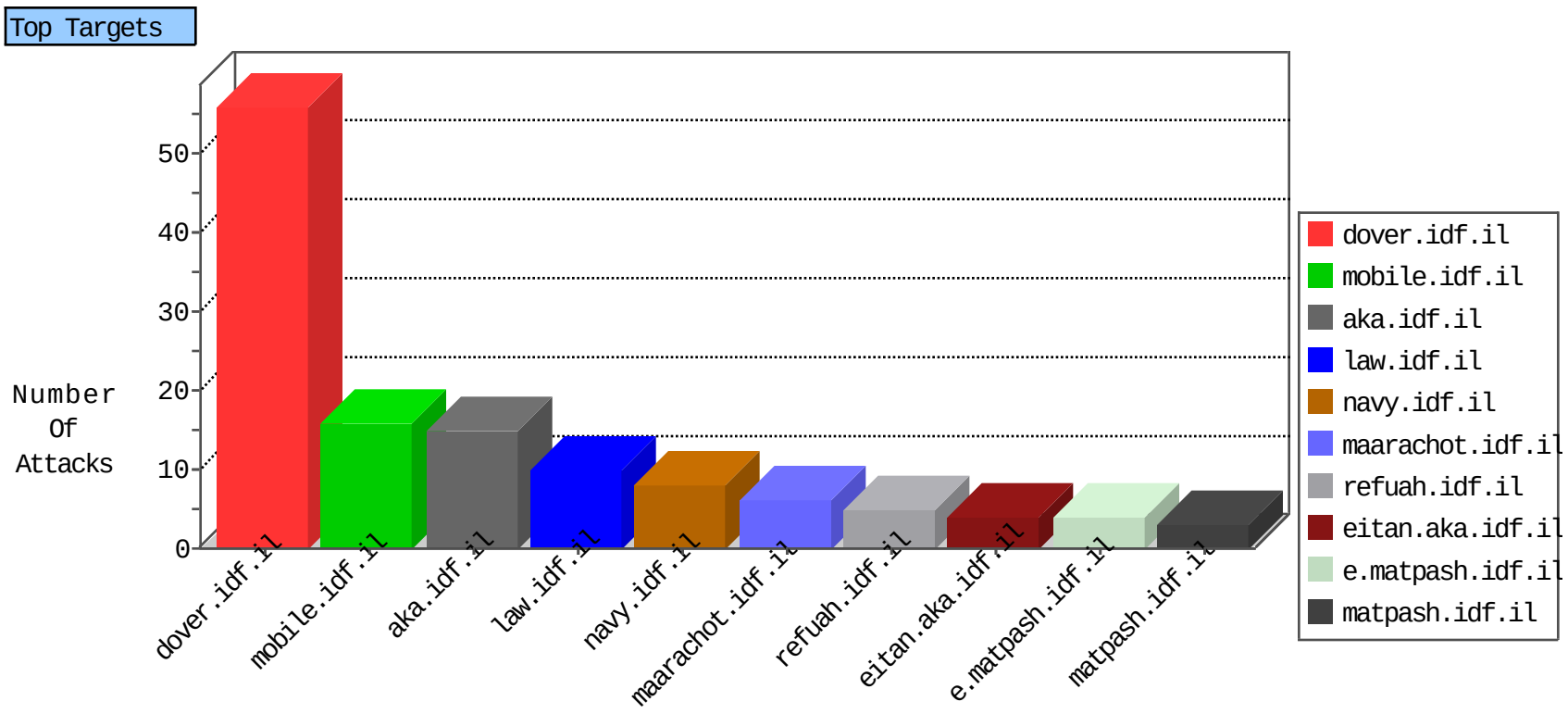
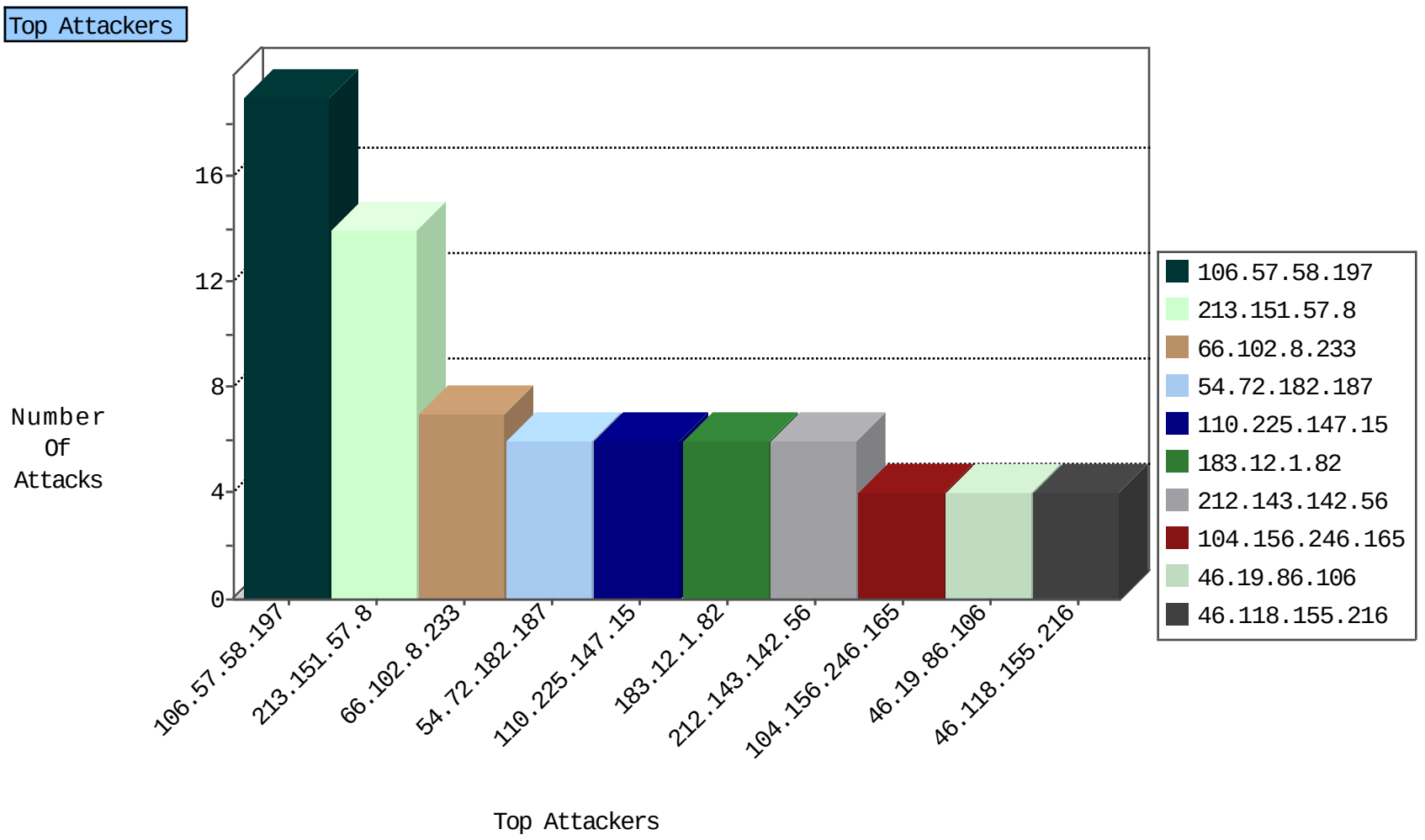
03-09-2016-04:04:06 to 03-09-2016-05:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-09-2016-04:04:06 to 03-09-2016-05:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
216.218.206.119	United States	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	1
104.156.246.165	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.250	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
104.156.246.165	United States	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.228		147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	1
104.156.246.165	United States	147.237.8.45	e.eitan.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.198	United States	147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1
23.228.107.104	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
216.218.206.119	United States	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1
104.156.246.165	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.214	United States	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	1

03-09-2016-04:04:06 to 03-09-2016-05:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.65.57	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
37.187.95.32	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
37.187.95.45	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
51.255.65.20	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-09-2016-04:04:06 to 03-09-2016-05:04:06

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	2
106.57.58.197	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
66.249.66.36	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.75.231	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
106.57.58.197	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
106.57.58.197	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.77.212	Canada	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
106.57.58.197	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
106.57.58.197	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
106.57.58.197	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
106.57.58.197	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
106.57.58.197	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.245	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 2048	1
106.57.58.197	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.245	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -f -sS	1
106.57.58.197	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
106.57.58.197	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
106.57.58.197	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
106.57.58.197	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
106.57.58.197	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
106.57.58.197	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
106.57.58.197	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
106.57.58.197	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
106.57.58.197	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.245	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1

03-09-2016-04:04:06 to 03-09-2016-05:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
213.151.57.8	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
110.225.147.15	India	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.106	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
94.254.129.180	Poland	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.11.50	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
183.12.1.82	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
79.179.31.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
183.12.1.82	China	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	2
183.206.168.57	China	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
108.162.156.157	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.22.134.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
144.76.93.46	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
184.105.139.75	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.213	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
137.116.71.170	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.18	United States	147.237.0.33	idf.il	drop		drop	1
184.105.247.231	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.218	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
49.195.22.179	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.120	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.208	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.35	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
188.120.148.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.219	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
67.243.31.139	United States	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
183.206.168.57	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
141.212.122.209	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.40	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
212.47.246.187	France	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
67.243.31.139	United States	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
183.206.168.57	China	147.237.77.243	mobile.idf.il	drop	SAM rule	drop	1
141.212.122.212	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.44	United States	147.237.0.35	akaws.idf.il	drop		drop	1
46.19.86.106	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
137.116.71.170	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.18	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

03-09-2016-04:04:06 to 03-09-2016-05:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
46.118.155.216	Ukraine	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
183.206.160.57	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/editor/editor/	Block	2
183.206.160.57	China	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/editor/editor/	Block	1
66.249.65.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
188.165.233.228	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
157.55.39.170	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
184.105.247.195	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.66.125	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/sip_storage/files/0/1350.pdf	Block	1
17.142.157.175	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
190.42.120.213	Peru	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
183.12.1.82	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
185.82.200.91		147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
70.181.5.157	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
195.154.243.14	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
183.206.160.57	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 183.206.160.57	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
185.82.200.91		147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
108.54.105.4	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.118.155.216	Ukraine	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
199.30.24.116	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.65.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
188.165.233.228	France	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 188.165.233.228	Block	1
141.212.122.209	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1

03-09-2016-04:04:06 to 03-09-2016-05:04:06