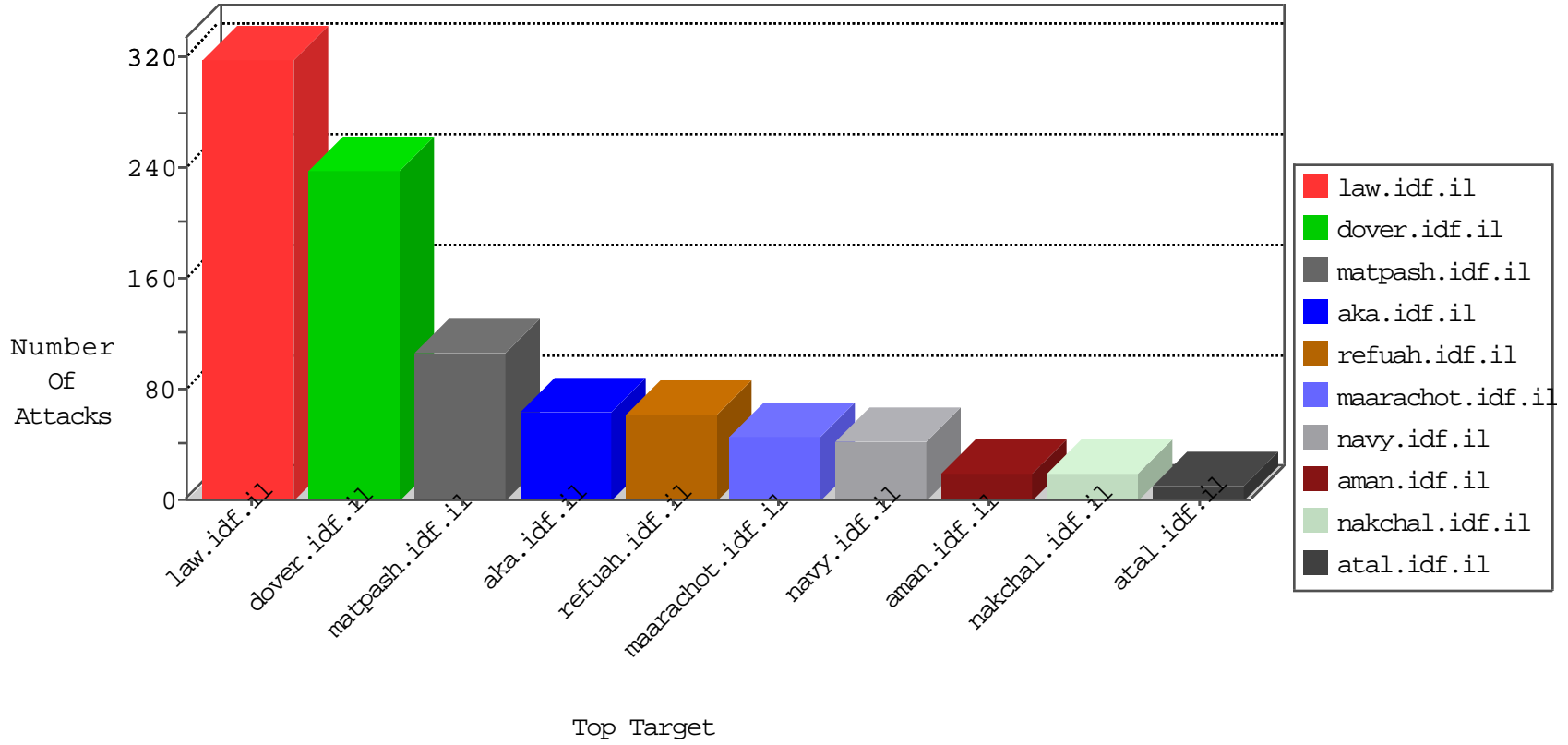
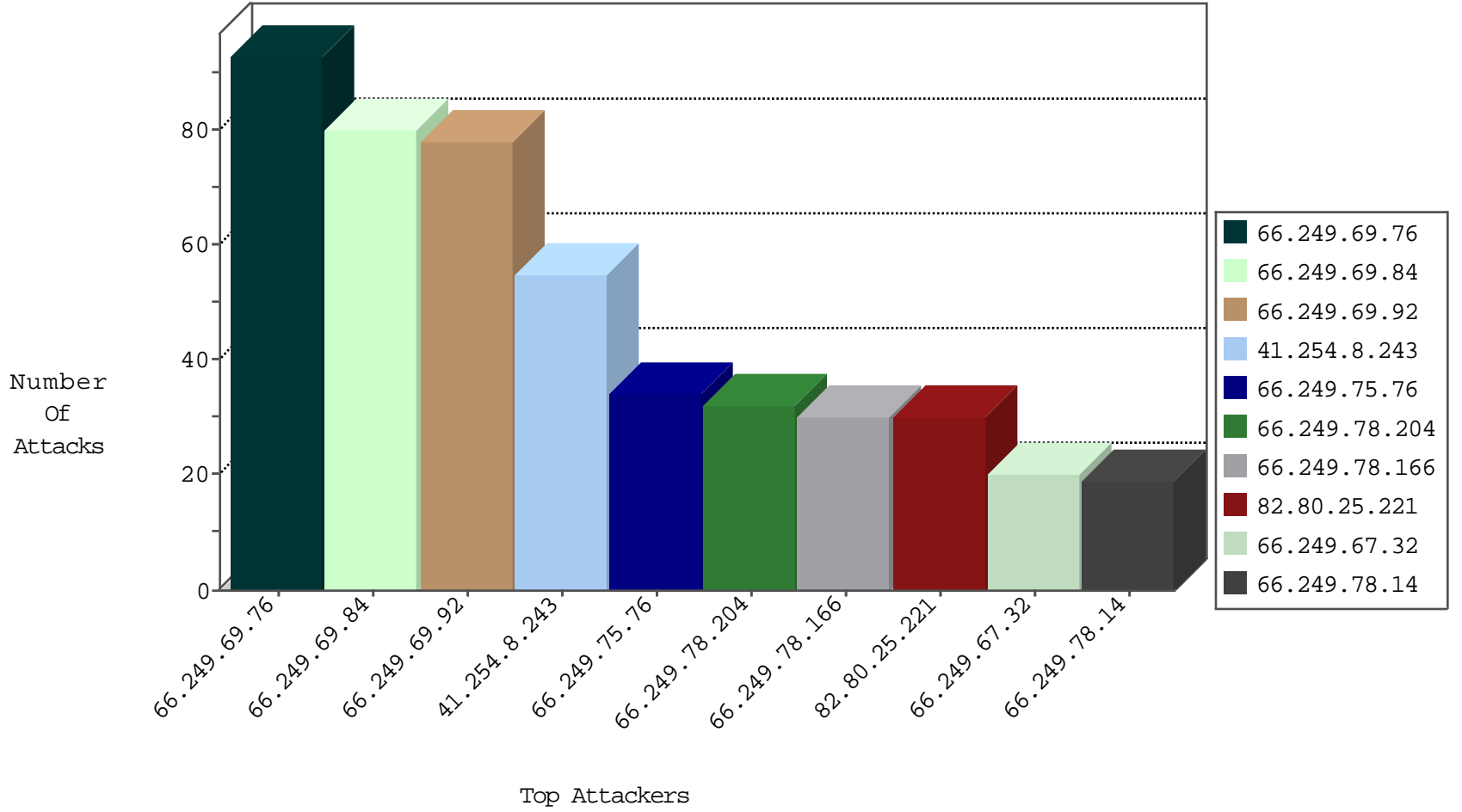




Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.69.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	93
66.249.69.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	78
66.249.69.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	75
66.249.75.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	34
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	32
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	30
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	20
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	19
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	19
66.249.75.68	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	18
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	17
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	16
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	14
66.249.64.114	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	14
66.249.78.198	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	12
66.249.64.118	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	12
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	12
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	12
66.249.64.110	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	12
66.249.75.60	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	11
66.249.67.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	9
66.249.67.5	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.67.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
66.249.67.157	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.75.103	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	7
66.249.67.34	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.67.24	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	6
66.249.75.95	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	5
66.249.67.13	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
66.249.75.69	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
66.249.65.146	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	5
66.249.67.39	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	4
66.249.64.41	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	4
66.249.78.54	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	4
66.249.67.66	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
66.249.78.120	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	3
66.249.75.113	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	3
66.249.78.160	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	3
66.249.75.9	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	3
66.249.67.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	3
66.249.75.111	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	3
66.249.67.26	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	2
66.249.64.136	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	2
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	2
66.249.64.167	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	2

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.25.103.50	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
46.172.229.241	Ukraine	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
149.88.106.54	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.254.20.38	Russian Federation	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	30
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
89.139.178.139	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
104.171.114.254		147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
95.110.213.46	Italy	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
87.236.215.124	United Kingdom	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
193.107.17.72	Russian Federation	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
188.138.9.51	Germany	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
117.135.163.104	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
104.171.114.254		147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
104.171.114.254		147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
95.110.213.46	Italy	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
87.236.215.124	United Kingdom	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243		147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
193.107.17.72	Russian Federation	147.237.77.234	halag.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
178.19.107.114	Poland	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
117.135.163.104	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -f -sS	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
41.254.8.243	Libyan Arab Jamahiriya	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	37
41.254.8.243	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
94.98.38.148	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
176.12.150.183	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.145.7	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
5.102.254.129	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
67.44.201.18	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
67.44.201.18	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
88.217.181.99	Germany	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	3
155.94.254.133		147.237.0.33	idf.il		drop	drop	2
188.165.15.198	France	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
2.54.146.132	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
2.54.146.132	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
2.54.146.132	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
141.212.122.193	United States	147.237.77.121	e.navy.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
188.165.15.29	France	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	1
46.19.85.111	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
109.253.138.165	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
174.236.161.241	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
198.20.69.74	United States	147.237.76.201	e.atal.idf.il	SAM rule	drop	drop	1
141.212.122.48	United States	147.237.76.202	e.halag.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
213.151.172.135	France	147.237.77.176	matpash.idf.il	header rejection pattern found in request	Header Rejection	monitor	1
141.212.122.187	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	1

04-04-2015-02:03:05 to 04-04-2015-03:03:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
136.243.36.97	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 136.243.36.97	Block	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
188.165.15.198	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1117-8.stm	Block	1
213.151.172.135	France	147.237.77.176	matpash.idf.il	eMail Hoarding	Block	1
188.165.15.238	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8833-he/refuah.aspx	Block	1
79.183.115.8	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
136.243.36.97	Germany	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
46.19.123.125	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
203.133.169.157	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
84.109.96.215	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00\$ctl00\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/gyus/atuda/asmachta.aspx	None	1
136.243.36.97	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
46.116.86.214	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/gyus/default.aspx	None	1
207.46.13.5	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorttype in aka.idf.il/eitan/listpage/	None	1
93.173.19.165	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
188.165.15.198	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.198	Block	1
46.116.86.214	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/gyus/miyun/miyunprocessquestionnaire.aspx	None	1
213.151.172.135	France	147.237.77.176	matpash.idf.il	E-mail collector robots 14	Block	1
109.186.171.202	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

04-04-2015-02:03:05 to 04-04-2015-03:03:05