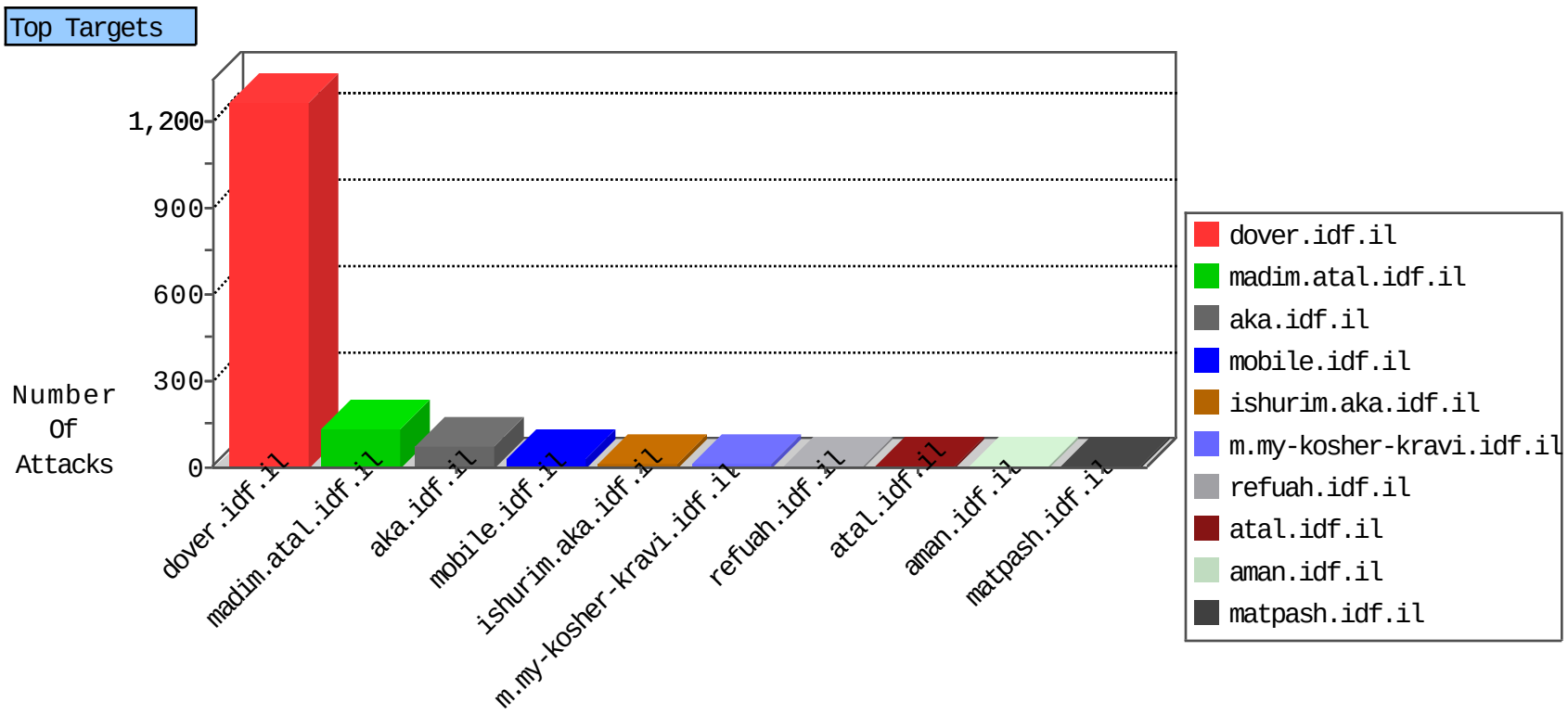
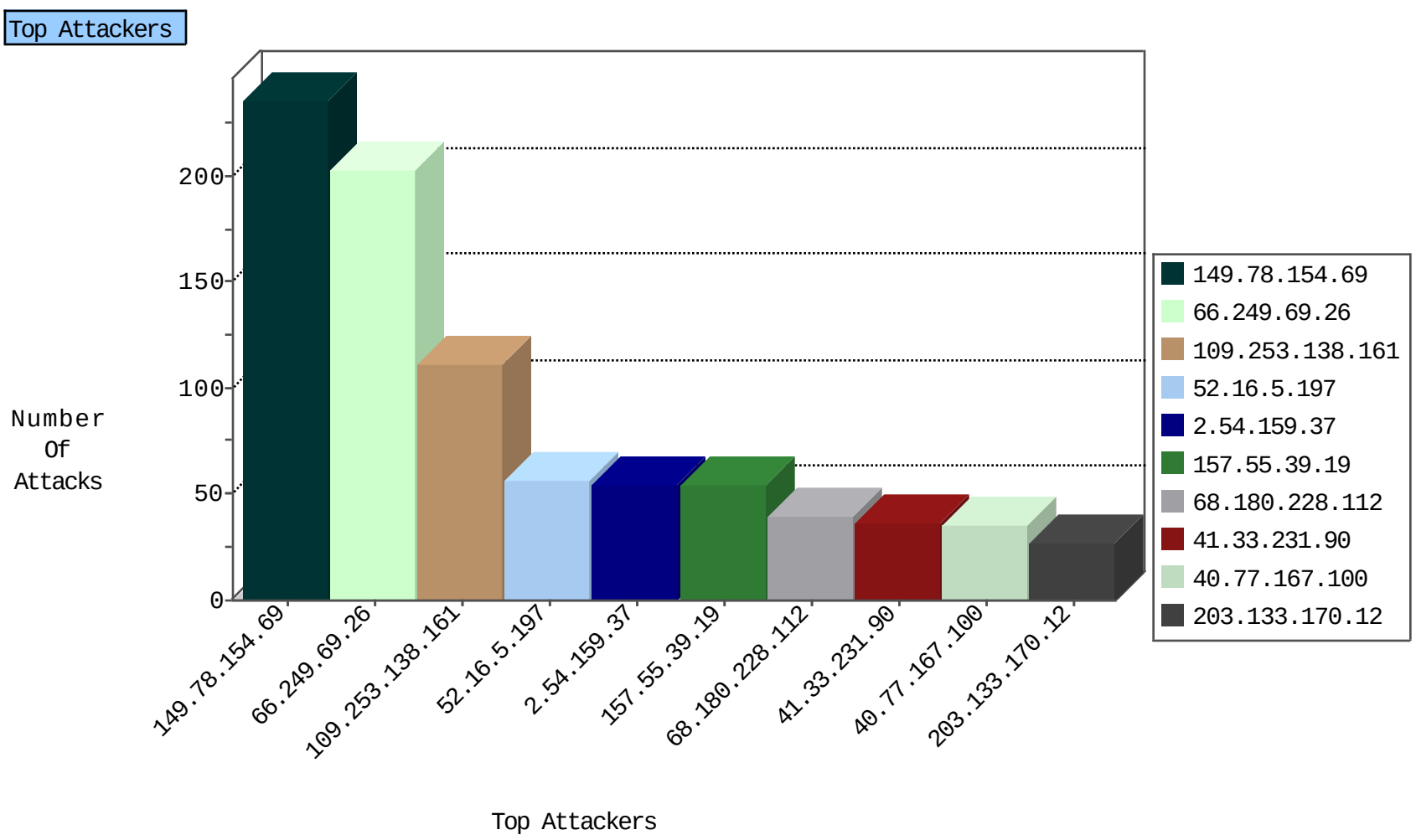
02-14-2016-06:04:06 to 02-14-2016-07:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-14-2016-06:04:06 to 02-14-2016-07:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	2
123.151.42.61	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	2
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
123.151.42.61	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
204.42.253.2	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
92.247.53.170	Bulgaria	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
92.247.53.170	Bulgaria	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

02-14-2016-06:04:06 to 02-14-2016-07:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
155.94.254.143	United States	147.237.77.170	maarachot.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
188.165.15.195	France	147.237.0.15	kosher-kravi.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-14-2016-06:04:06 to 02-14-2016-07:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.88.187	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
218.246.0.97	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
130.211.100.171	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.224.8	147.237.72.166	Ukraine	aka.idf.il	SERVER-WEBAPP admin.php access	1
130.211.100.171	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

02-14-2016-06:04:06 to 02-14-2016-07:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.26.149.237	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
176.13.3.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.141.206	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.252	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.42	Israel	147.237.77.243	mobile.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
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
77.125.81.238	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
87.69.48.54	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
176.13.22.59	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
157.55.39.155	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.30.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.50.1	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.200.205.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.37.228	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.204.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.61.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.28.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.38.251.62	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
82.166.140.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
66.249.66.60	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.54.134.152	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
2.54.190.61	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.108.145.241	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
2.54.190.61	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
203.133.168.41	Korea, Republic of	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
2.54.190.61	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
87.69.192.101	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.119	United States	147.237.0.33	idf.il	drop		drop	1
74.82.47.30	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
54.209.209.198	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.247.244	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.72	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
45.79.168.168		147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
5.22.134.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
93.113.125.11	Romania	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.124	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.34	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.185	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.244	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.94.24.239	Israel	147.237.0.15	kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.99	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
195.62.53.168	Russian Federation	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	234
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	201
109.253.138.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	77
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	56
2.54.159.37	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	54
157.55.39.19	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	53
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	40
40.77.167.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	35
109.253.138.161	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.138.161	Block	33
203.133.170.12	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	27
5.29.78.38	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	27
100.4.207.101	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
79.181.235.165	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
157.55.39.159	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
46.19.85.42	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
109.66.172.9	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
77.125.94.120	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	16
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
46.19.85.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
46.121.150.176	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.121.150.176	Block	11
46.19.86.169	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
195.200.205.2	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
79.177.203.167	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
45.35.64.142		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
54.167.183.116	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
109.253.134.80	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
176.13.20.171	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
2.52.165.23	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
176.13.8.119	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
2.54.134.152	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
205.203.135.1	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
82.166.112.120	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
85.250.101.6	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
87.68.145.168	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
2.54.20.32	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
176.13.22.59	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
37.26.147.148	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
2.54.28.82	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
212.235.98.139	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
2.52.165.255	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
24.130.83.75	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
107.170.78.137	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
87.70.6.85	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
209.133.111.211	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3

02-14-2016-06:04:06 to 02-14-2016-07:04:06