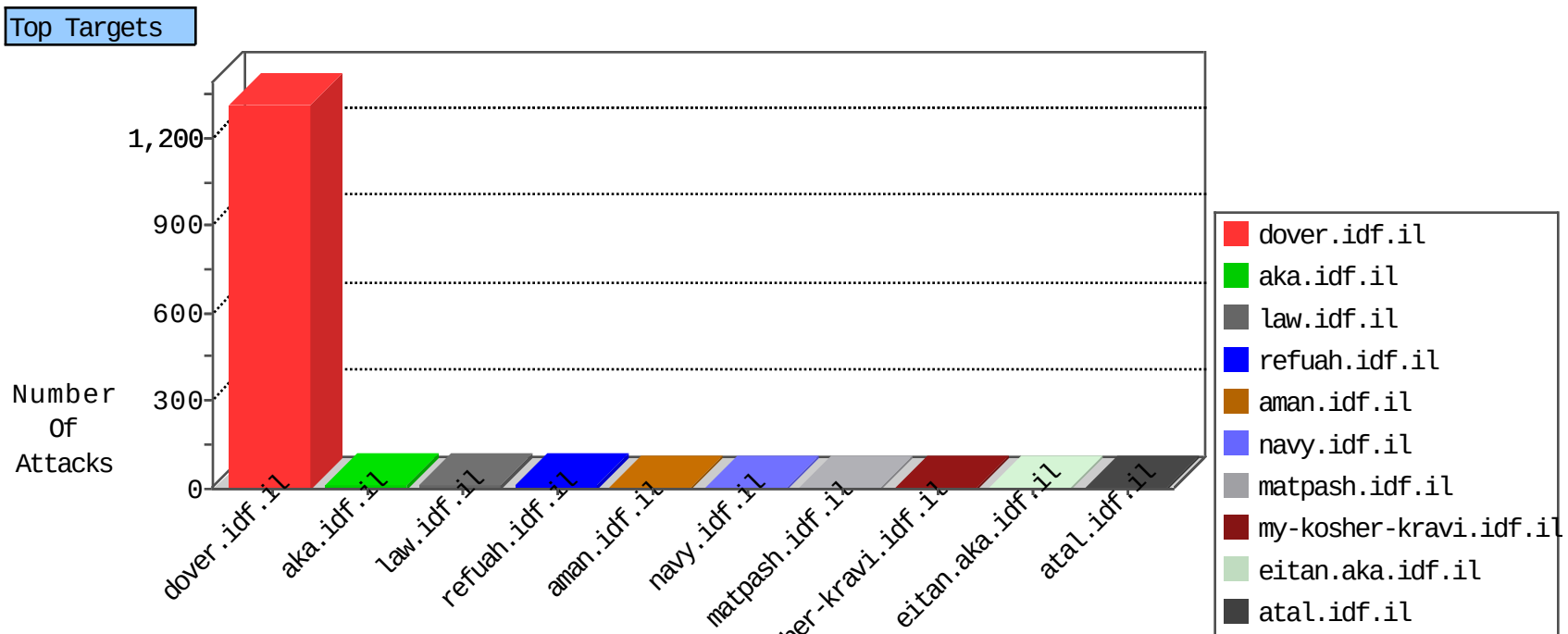
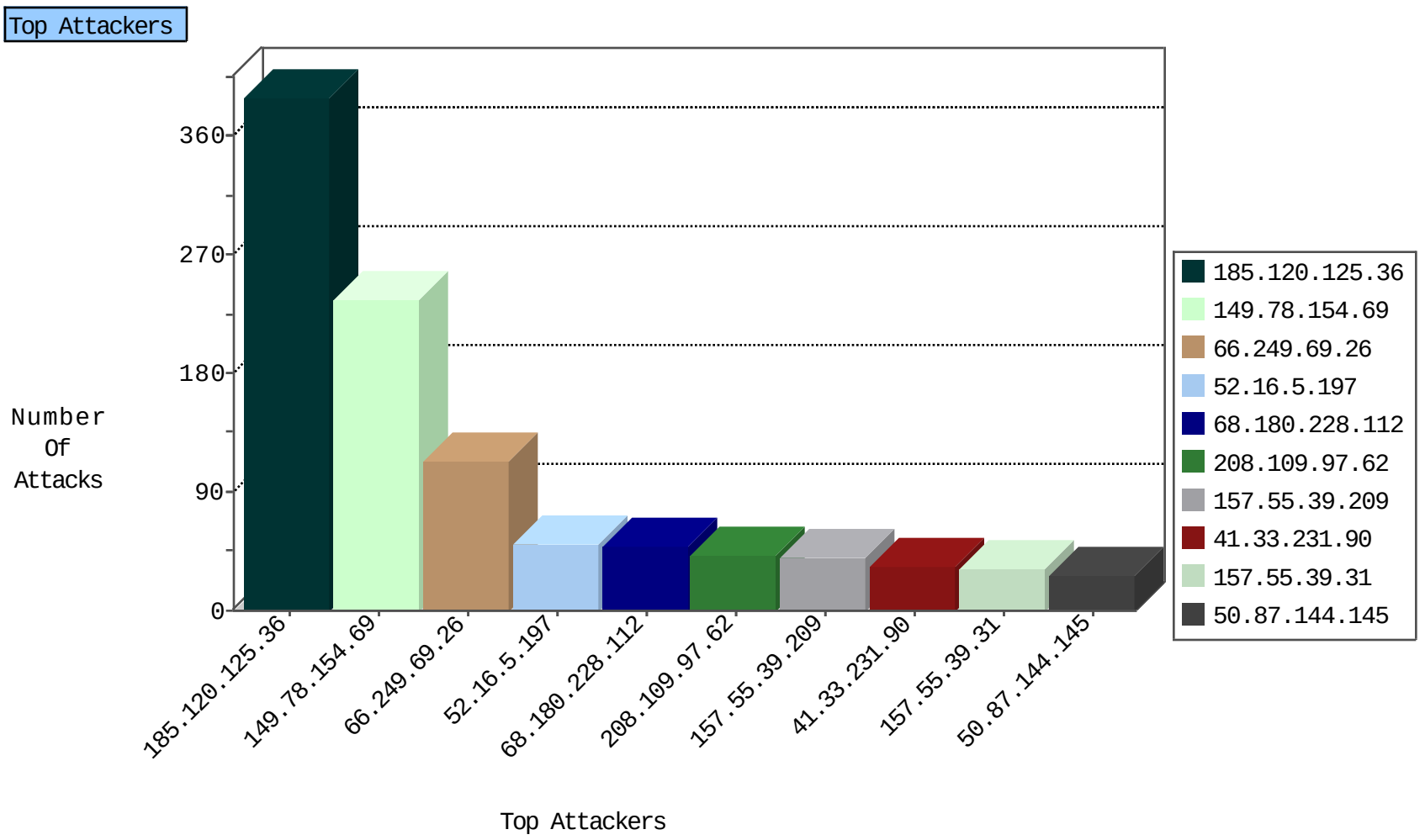
02-13-2016-07:04:01 to 02-13-2016-08:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-13-2016-07:04:01 to 02-13-2016-08:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.5.224		147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
50.23.64.17	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

02-13-2016-07:04:01 to 02-13-2016-08:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.97.83.125	Switzerland	147.237.76.42	refuah.idf.il	14331: HTTP: Suspicious User-Agent (My Session)	Block	1
195.154.181.168	France	147.237.77.216	dover.idf.il	22611: HTTP: WordPress LoginWall Fake Plugin Usage	Block	1
198.20.69.74	United States	147.237.8.24	e.lifestyle.idf.i	13840: TLS: OpenSSL Heartbeat Packet	Block	1

02-13-2016-07:04:01 to 02-13-2016-08:04:01

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	3
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.235.254.181	147.237.77.61	Turkey	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
104.128.144.131	147.237.72.156	Canada	aman.idf.il	ET SCAN NMAP -sS window 2048	1
93.174.95.102	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.184.195.114	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.231	147.237.77.74		law.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.231	147.237.8.28		e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
112.234.22.231	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.235.254.181	147.237.77.61	Turkey	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.72.156	Canada	aman.idf.il	ET SCAN NMAP -f -sS	1
93.174.95.102	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.231	147.237.8.45		e.eitan.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1

02-13-2016-07:04:01 to 02-13-2016-08:04:01

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	34
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
80.179.202.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
178.255.215.87	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
176.77.51.169	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.22.135.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
84.94.24.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.65.136.82	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
199.168.142.24	United States	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
141.212.122.201	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
104.128.144.131	Canada	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.220	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.206	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.195	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.65.136.82	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
204.17.56.42	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
71.6.167.142	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.202	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.220	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.207	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.196	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
93.174.93.218	Netherlands	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.43	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.76.15.16	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.203	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.110.34.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.207	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.197	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.174.93.218	Netherlands	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.80	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
27.63.181.69	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.204	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.8.132.32	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
84.110.34.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
199.168.142.24	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
149.78.94.24	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.198	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
96.226.75.73	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.215	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
27.63.181.69	India	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.206	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.120.125.36		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	388
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	113
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	50
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	49
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
157.55.39.209	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	40
157.55.39.31	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	31
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	25
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
17.142.156.109	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	21
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
149.88.7.196	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
80.179.202.211	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
45.35.64.142		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
109.66.97.108	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
197.38.218.170	Egypt	147.237.77.74	law.idf.il	PHP Attempt	Block	5
84.111.138.75	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
197.38.218.170	Egypt	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	5
176.13.14.183	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
46.120.73.197	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
169.0.183.214		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
46.120.130.84	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
131.253.25.155	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
205.203.135.1	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
125.84.185.102	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
93.173.162.94	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
79.180.50.121	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
66.220.146.180	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
181.192.0.137	Argentina	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
104.166.52.234	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
65.55.210.192	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
156.197.96.171		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
40.143.1.4	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
109.67.203.121	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
79.179.142.118	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.9	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	2
87.203.103.161	Greece	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
46.117.128.81	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
8.29.198.25	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
199.16.156.125	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
149.78.87.160	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
109.186.180.239	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
81.218.181.240	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
85.64.113.244	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
199.59.148.210	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
66.220.146.182	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
89.139.141.217	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
27.63.181.69	India	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2

02-13-2016-07:04:01 to 02-13-2016-08:04:01