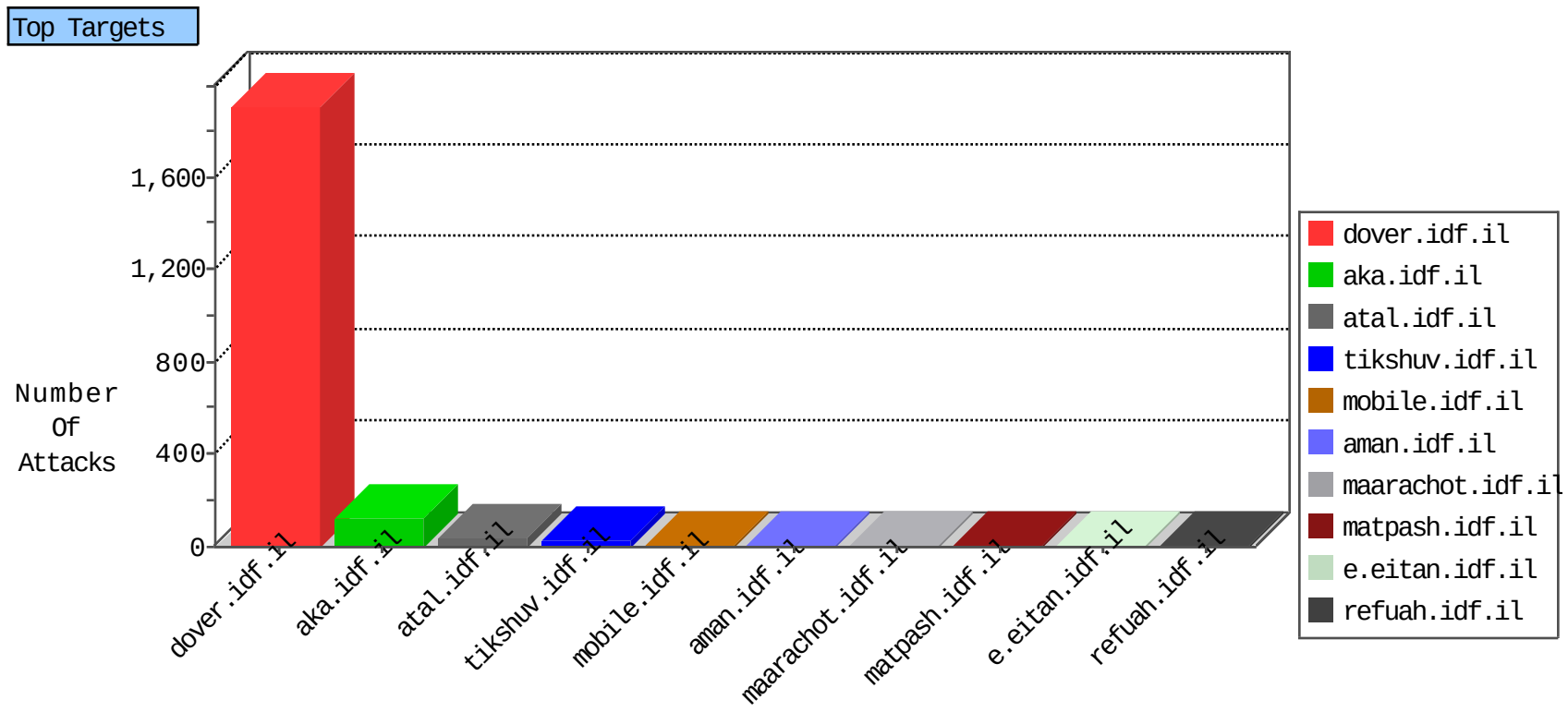
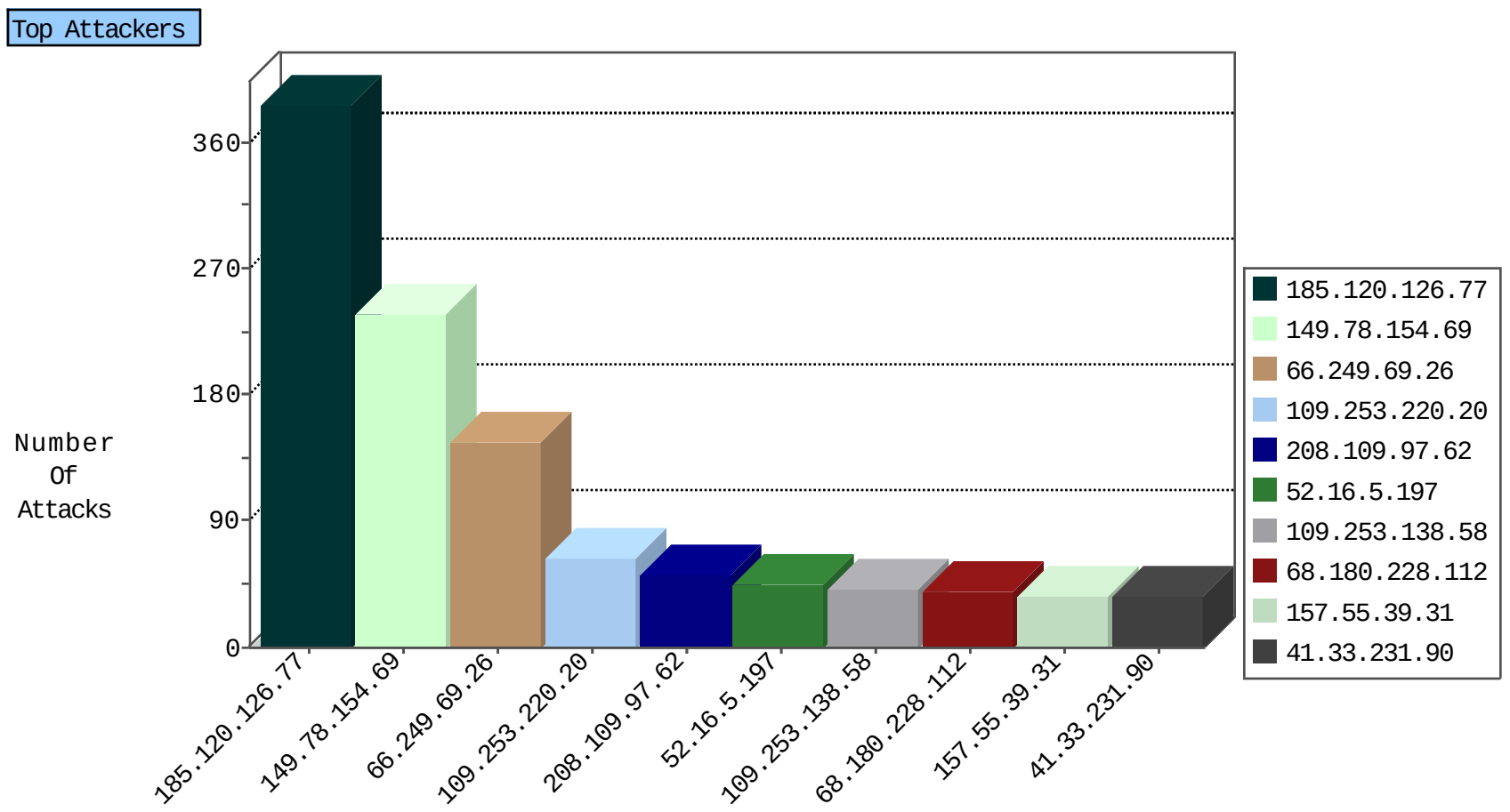
02-13-2016-11:04:01 to 02-13-2016-12:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-13-2016-11:04:01 to 02-13-2016-12:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
158.130.6.191	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
66.249.64.41	Israel	147.237.0.16	my-kosher-kravi.idf.il	TCP handshake violation, first packet not syn	drop	1
79.176.4.235	Israel	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1

02-13-2016-11:04:01 to 02-13-2016-12:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.216.115.8		147.237.77.216	dover.idf.i	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	2

02-13-2016-11:04:01 to 02-13-2016-12:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
50.204.188.142	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
211.215.19.235	147.237.8.50	Korea, Republic of	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
31.184.195.114	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.215.19.235	147.237.8.45	Korea, Republic of	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
211.215.19.235	147.237.8.24	Korea, Republic of	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
125.212.232.146	147.237.76.39	Vietnam	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
50.204.188.142	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
211.215.19.235	147.237.8.46	Korea, Republic of	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
211.215.19.235	147.237.8.27	Korea, Republic of	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
125.212.232.146	147.237.76.39	Vietnam	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
114.112.90.54	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

02-13-2016-11:04:01 to 02-13-2016-12:04:01

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	36
37.26.148.255	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	30
185.120.126.31		147.237.72.166	aka.idf.il	drop	SAM rule	drop	24
46.19.86.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
109.253.138.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
87.69.55.159	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
80.246.136.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.130.253	Israel	147.237.72.166	aka.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
109.253.138.58	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.20.160	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
109.64.20.160	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
31.154.149.23	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.22.131.68	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
178.255.215.87	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
212.227.100.244	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.179.5.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.180.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.75.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.176.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.30.135	Israel	147.237.77.243	mobile.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
46.19.85.90	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.180.120.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.8.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.138.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.72.178	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
66.102.9.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	3
93.158.152.49	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.54.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.107.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.114	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
5.22.131.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
208.109.97.62	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
213.8.204.12	Israel	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
188.120.148.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.90	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
68.180.229.173	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.86.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
31.210.186.17	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.131.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
62.210.132.11	France	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
212.179.57.94	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.102.9.127	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
169.229.3.91	United States	147.237.72.14	dover.idf.il(old)	drop	SAM rule	drop	1
66.240.192.138	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.120.126.77		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	385
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	236
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	146
109.253.220.20	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	64
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	50
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	44
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	38
157.55.39.31	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	37
157.55.39.209	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	32
77.125.90.116	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
109.253.138.58	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
46.19.85.238	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
82.205.113.88	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
93.172.36.187	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	19
37.201.213.71	Germany	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
188.120.148.54	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
5.102.207.164	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
84.111.23.42	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
149.78.254.185	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
80.246.137.5	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
84.228.244.116	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
77.126.255.208	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
176.13.21.204	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
84.228.19.253	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
91.240.80.25	Lebanon	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
45.35.64.142		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
85.65.155.101	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
79.182.130.105	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
37.26.146.239	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
84.229.135.34	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
2.54.146.248	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
87.69.55.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
46.19.86.59	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
176.13.11.218	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
176.13.15.188	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
79.181.144.202	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
109.66.173.130	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
79.178.130.15	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
217.132.52.149	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.143	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
176.13.10.23	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
184.153.75.12	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
49.177.22.136	Australia	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
77.127.199.63	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
109.253.132.14	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
85.250.180.5	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4

02-13-2016-11:04:01 to 02-13-2016-12:04:01