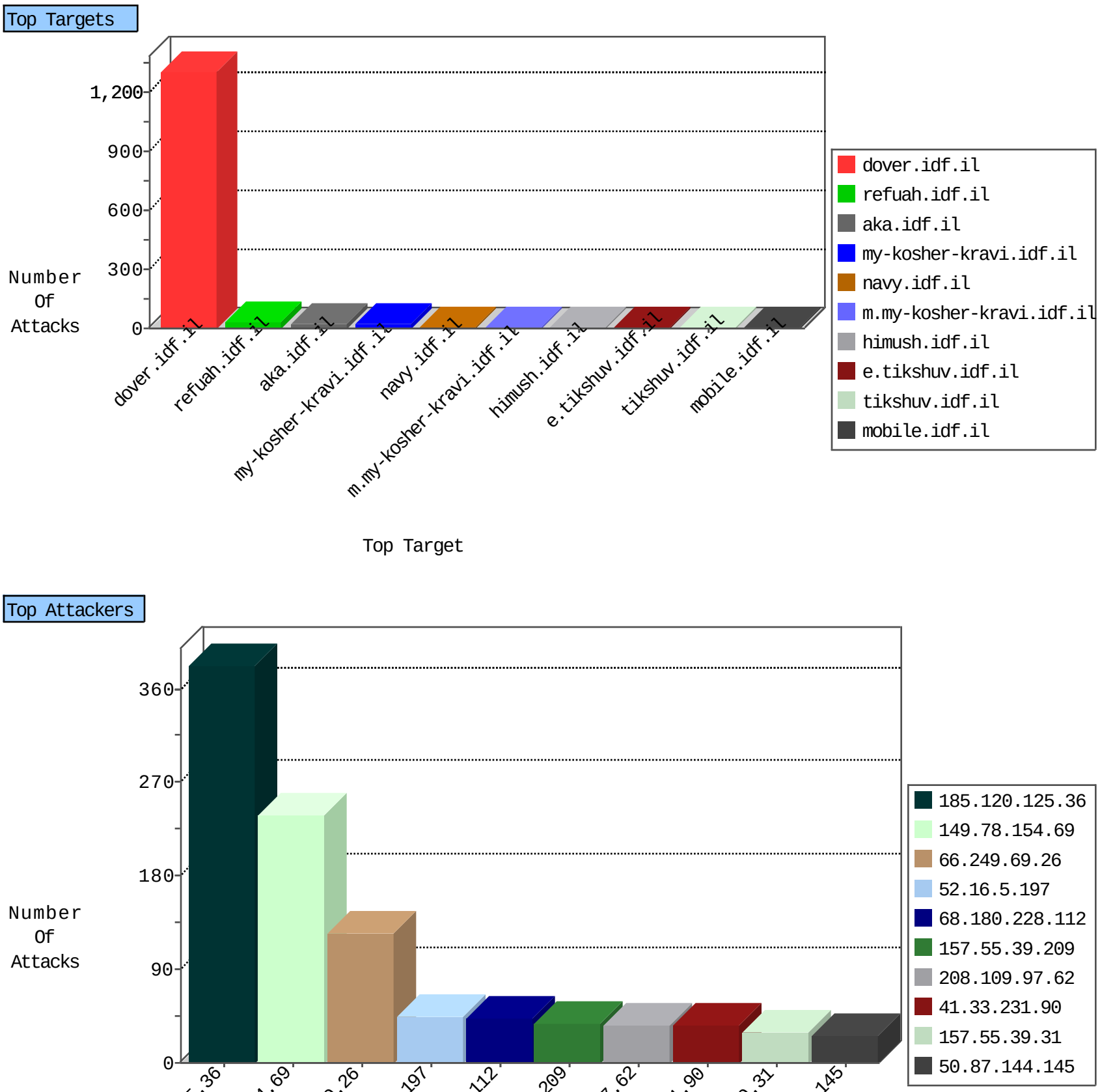
02-13-2016-06:04:04 to 02-13-2016-07:04:04

IDF Under Attack Daily Report



02-13-2016-06:04:04 to 02-13-2016-07:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.127	Israel	147.237.0.16	my-kosher-kravi.idf.il	TCP handshake violation, first packet not syn	drop	1738
111.73.45.122	China	147.237.0.17	m.my-kosher-kravi.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
42.98.179.49	Hong Kong	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
85.25.43.94	Germany	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

02-13-2016-06:04:04 to 02-13-2016-07:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.209	France	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-13-2016-06:04:04 to 02-13-2016-07:04:04

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	4
185.130.5.231	147.237.0.35		akaws.idf.il	ET SCAN Potential SSH Scan	1
183.61.109.189	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 4096	1
119.40.88.226	147.237.0.34	Bangladesh	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
119.40.88.226	147.237.0.34	Bangladesh	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
185.130.5.231	147.237.77.212		e.dover.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.231	147.237.76.198		e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.244.111.77	147.237.76.148	Hong Kong	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.231	147.237.76.176		test.ncore.idf.il	ET SCAN Potential SSH Scan	1
61.244.111.77	147.237.0.19	Hong Kong	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.231	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.231	147.237.72.166		aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.231	147.237.0.15		kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
121.201.27.61	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
119.40.88.226	147.237.0.34	Bangladesh	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
185.130.5.231	147.237.77.233		atal.idf.il	ET SCAN Potential SSH Scan	1
114.215.111.222	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.231	147.237.76.201		e.atal.idf.il	ET SCAN Potential SSH Scan	1
61.244.111.77	147.237.76.176	Hong Kong	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.231	147.237.76.177		ncore.idf.il	ET SCAN Potential SSH Scan	1
61.244.111.77	147.237.76.147	Hong Kong	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.231	147.237.76.42		refuah.idf.il	ET SCAN Potential SSH Scan	1
31.184.195.114	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.231	147.237.76.30		himush.idf.il	ET SCAN Potential SSH Scan	1

02-13-2016-06:04:04 to 02-13-2016-07:04:04

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
37.46.39.29	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
82.166.115.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
207.8.49.34	United States	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	5
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.88.165.73	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
178.255.215.87	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
71.185.26.254	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
157.55.39.161	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.183.199.135	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
54.193.80.215	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
178.255.215.87	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
141.212.122.202	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.24	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.92	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.203	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.27	United States	147.237.0.35	akaws.idf.il	drop		drop	1
216.218.206.86	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.123	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
157.55.39.55	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
94.23.36.99	France	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
195.66.76.4	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
37.46.39.29	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.75	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.204	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.43	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.86	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.224	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.176	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.6	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
198.20.69.74	United States	147.237.8.24	e.lifestyle.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.78	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.205	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.46	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.228	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.191	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.8	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.46.39.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.88	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.78.94.24	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
82.166.115.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
188.138.1.218	Germany	147.237.76.30	himush.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	382
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	235
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	121
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	41
157.55.39.209	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	36
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	36
157.55.39.31	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	29
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
5.28.159.226	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
79.176.23.128	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
68.195.72.213	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
207.8.49.34	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
71.185.26.254	United States	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	9
2.88.165.73	Saudi Arabia	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
2.54.56.114	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
2.54.183.35	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
37.26.149.150	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
79.179.227.201	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
5.28.146.67	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
130.154.0.250	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
184.153.75.12	United States	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
205.203.135.1	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
162.243.57.54	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	3
131.253.25.209	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
128.242.249.11	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
8.37.70.237	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
2.54.34.216	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
176.13.9.236	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.110	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
8.37.234.3	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
79.180.213.152	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
109.253.202.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
104.131.226.73	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
75.80.245.134	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.157	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
104.180.45.243	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
182.253.24.171	Indonesia	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
5.29.93.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
108.210.29.159	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
199.30.24.75	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
124.217.249.254	Malaysia	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
5.29.143.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2

02-13-2016-06:04:04 to 02-13-2016-07:04:04