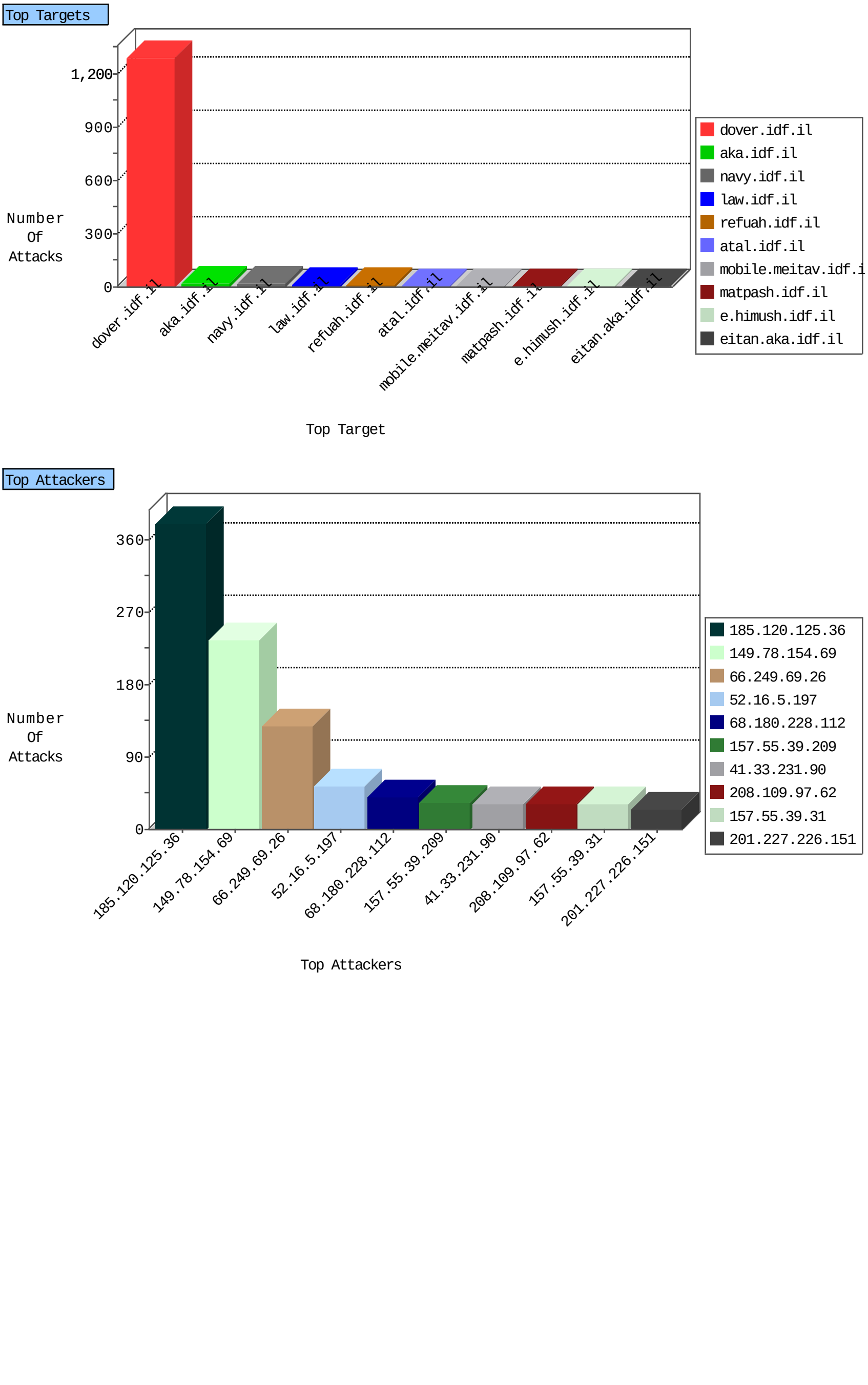
02-13-2016-05:04:01 to 02-13-2016-06:04:01

IDF Under Attack Daily Report



02-13-2016-05:04:01 to 02-13-2016-06:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.94.111.1		147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

02-13-2016-05:04:01 to 02-13-2016-06:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.159	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

02-13-2016-05:04:01 to 02-13-2016-06:04:01

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	4
175.99.87.209	147.237.77.61	Taiwan	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
93.113.125.11	147.237.76.176	Romania	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
45.79.10.124	147.237.76.39		mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
175.99.87.209	147.237.77.61	Taiwan	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
114.112.90.54	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.195.114	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
198.20.69.74	147.237.77.74	United States	law.idf.il	ET DROP Dshield Block Listed Source	1
185.130.5.231	147.237.77.233		atal.idf.il	ET SCAN NMAP -sS window 1024	1

02-13-2016-05:04:01 to 02-13-2016-06:04:01

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	32
201.227.226.151	Panama	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
178.255.215.87	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.188.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
178.255.215.87	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
207.46.13.55	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.46.13.123	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
199.30.24.129	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
75.126.221.55	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
75.126.221.55	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
45.79.10.124		147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
75.126.221.55	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
141.212.122.178	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.118	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
199.255.138.45	United States	147.237.77.74	law.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
184.105.139.112	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.179	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
72.192.147.154	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
199.255.138.45	United States	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
184.105.139.116	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.199	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.28	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
199.168.142.24	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
201.227.226.151	Panama	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.203	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.200	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.104	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
199.255.138.45	United States	147.237.72.166	aka.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
184.105.139.82	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.105.247.240	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
173.236.152.135	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
216.218.206.110	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.54.155.96	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
199.255.138.45	United States	147.237.76.42	refuah.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
184.105.139.92	United States	147.237.8.50	e.tikshuv.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
185.120.125.36		147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	381
149.78.154.69	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	236
66.249.69.26	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	119
52.16.5.197	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	54
68.180.228.112	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	40
157.55.39.209	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	34
208.109.97.62	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	32
157.55.39.31	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	29
50.87.144.145	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	25
192.249.66.247	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	24
84.108.32.84	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	22
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	18
87.71.1.59	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	15
82.80.25.221	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	12
66.249.69.26	Israel	147.237.77.216	dover.idf.i	Multiple Unauthorized URL Access from 66.249.69.26	Block	9
45.35.64.142		147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	8
66.249.69.34	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	8
109.67.49.203	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	7
79.178.196.147	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	6
89.139.150.24	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	6
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	5
2.54.177.45	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	4
169.0.183.214		147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	4
66.249.69.42	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	4
174.117.120.231	Canada	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	4
118.173.169.28	Thailand	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	3
84.94.25.35	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	3
162.243.57.54	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	3
104.162.241.87	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	3
37.187.162.184	France	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
109.253.194.114	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
199.30.25.34	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
8.37.71.74	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
179.155.252.112	Brazil	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
2.96.249.139	United Kingdom	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
205.203.135.1	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
107.170.119.178	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
79.178.39.130	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
5.29.121.5	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
207.8.49.34	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
108.29.8.15	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
5.102.242.131	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
198.58.102.96	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
176.13.2.223	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
84.108.105.69	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
66.249.91.14	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
2.52.158.218	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
65.19.138.34	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
8.29.198.25	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2

02-13-2016-05:04:01 to 02-13-2016-06:04:01