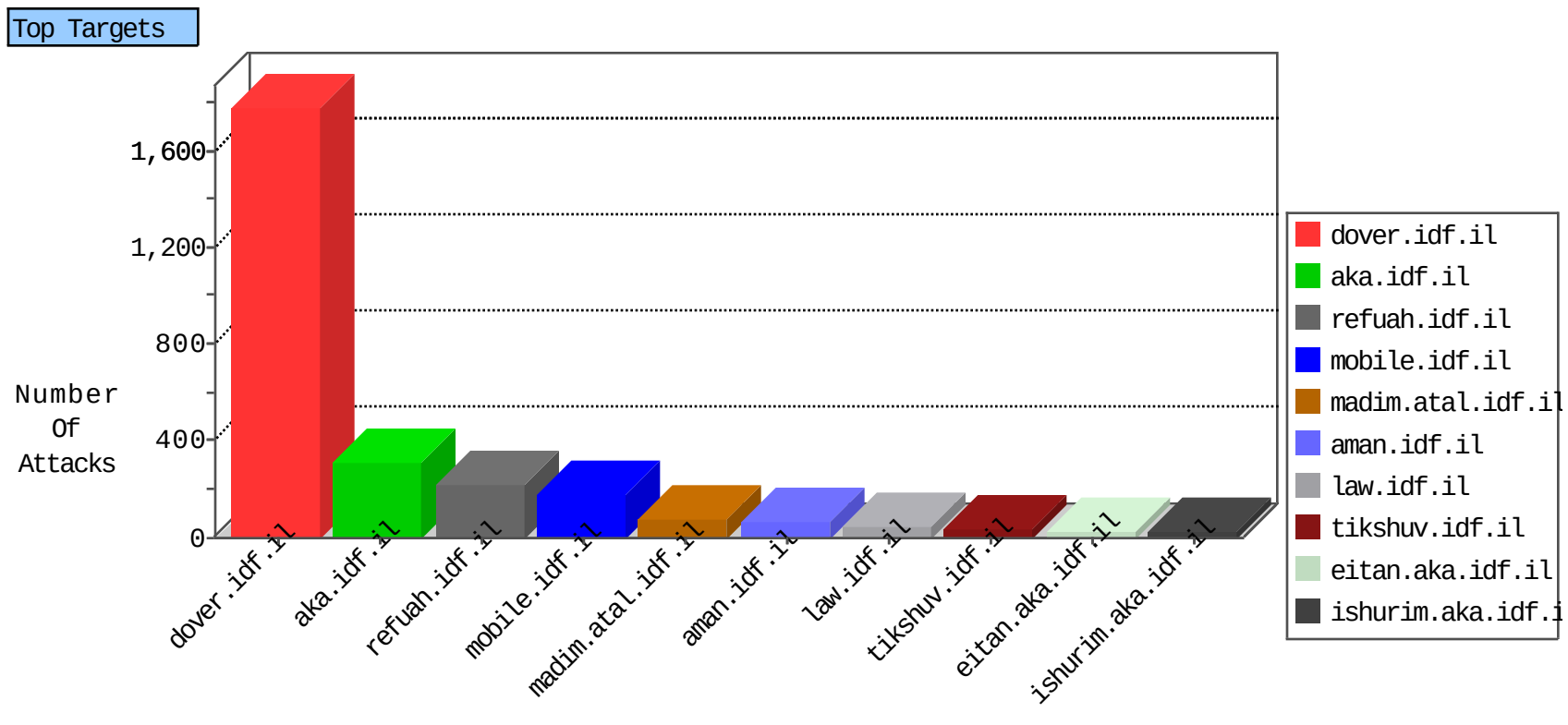
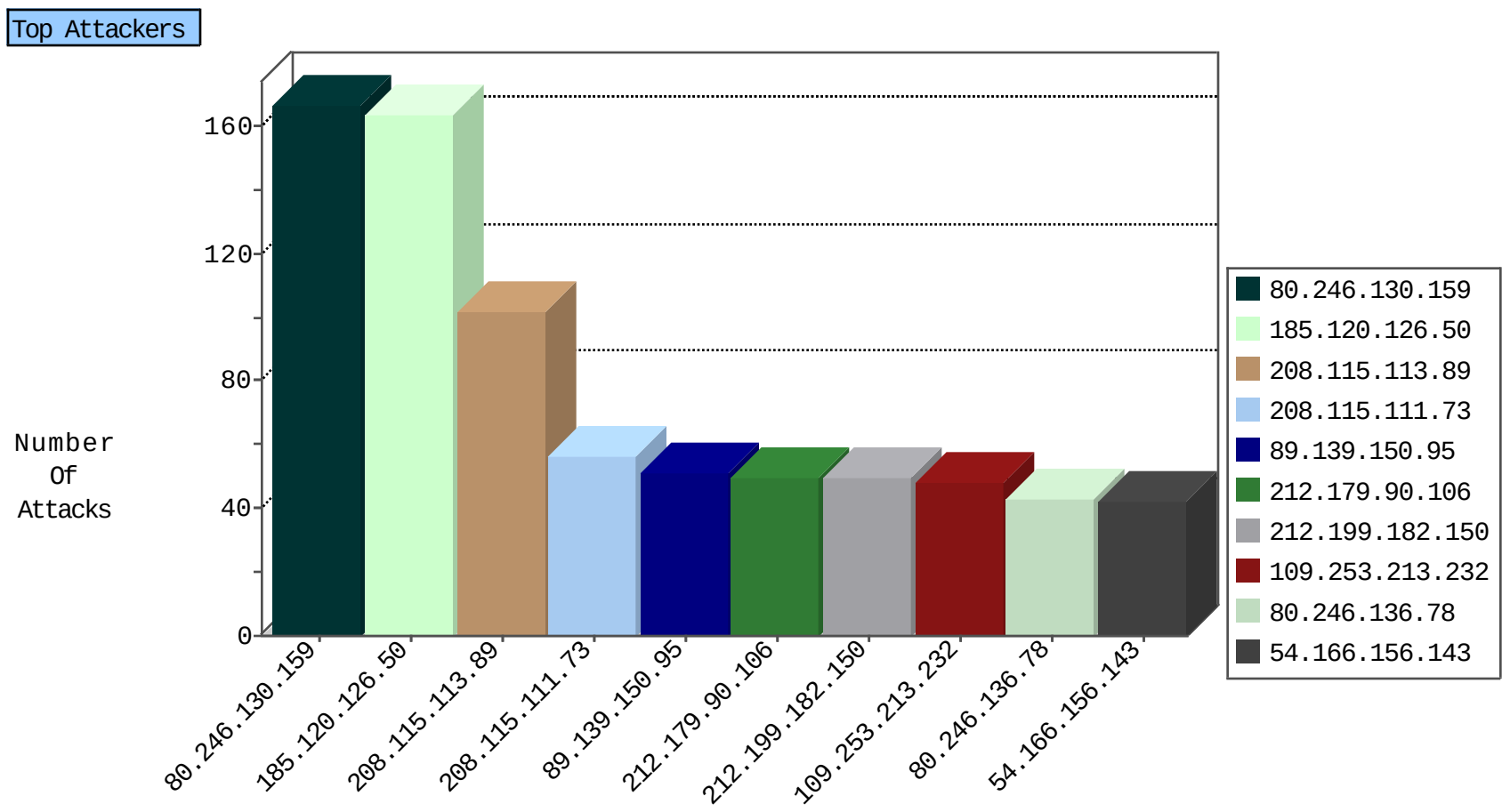
02-15-2016-16:04:07 to 02-15-2016-17:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-15-2016-16:04:07 to 02-15-2016-17:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
85.98.159.38	Turkey	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
139.196.34.205	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	2
93.158.203.154	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
173.208.206.202	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
93.158.203.154	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
107.150.60.74	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1

02-15-2016-16:04:07 to 02-15-2016-17:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.84.136.105	United States	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
216.185.43.135	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
216.185.43.135	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
184.173.233.226	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
93.63.188.181	Italy	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
184.173.233.226	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
64.31.44.6	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
96.48.22.37	Canada	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.246.49.97	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
74.84.136.105	United States	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
216.185.43.135	United States	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
152.115.70.227	Denmark	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
89.139.63.229	Israel	147.237.72.167	ishurim.aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
152.115.70.227	Denmark	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1

02-15-2016-16:04:07 to 02-15-2016-17:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
152.115.70.227	147.237.72.166	Denmark	aka.idf.il	SQL Injection - Select From	13
184.173.233.226	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	10
64.31.44.6	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	7
93.63.188.181	147.237.77.74	Italy	law.idf.il	SQL Injection - Select From	7
213.246.49.97	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	4
132.64.213.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.10.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.100.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.102.136.69	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
188.126.77.138	147.237.77.176	Sweden	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
183.82.106.200	147.237.76.196	India	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.249.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.95.209.243	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
75.147.243.2	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.8.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-15-2016-16:04:07 to 02-15-2016-17:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.130.159	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	166
54.166.156.143	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	42
80.246.136.78	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
54.166.166.103	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	36
54.145.187.192	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	35
54.145.174.23	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	34
2.52.58.78	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
54.221.36.192	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	27
109.253.141.143	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
109.66.144.158	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
54.204.103.55	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	21
109.253.158.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
54.166.175.191	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	19
79.182.103.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
173.241.185.194	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
109.253.205.120	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.253.142.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.138.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.100	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.50.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.147.207	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.147.231	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
17.78.79.134	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.86.186	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
66.102.9.3	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	7
177.185.194.45	Brazil	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
62.207.60.228	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
109.66.13.27	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
109.186.173.3	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.86.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.148.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.128.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.142.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.3.147.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.192.69.14	Morocco	147.237.77.216	dover.idf.il	drop		drop	5
79.182.126.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
31.210.186.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.29.40.70	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
213.57.177.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.199.156.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.46.38.173	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.114	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.148.3	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
109.67.42.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-15-2016-16:04:07 to 02-15-2016-17:04:07

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
37.26.148.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.120.126.50		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	164
208.115.113.89	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	102
208.115.111.73	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	56
212.179.90.106	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	50
212.199.182.150	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	50
109.253.213.232	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	48
89.139.150.95	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	46
176.13.5.7	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	41
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	37
46.19.85.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	29
37.26.149.181	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
80.246.136.253	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
194.90.25.90	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
46.19.85.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
157.55.39.32	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	17
37.46.38.20	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 37.46.38.20	Block	17
81.218.202.150	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	16
212.199.195.128	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/resource/userfollowresource/create/	Block	15
109.253.205.120	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
37.46.38.20	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
87.69.251.254	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
207.232.21.105	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
2.54.47.150	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
176.13.19.231	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
207.232.27.5	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
207.46.13.111	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
157.55.39.28	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
79.181.210.83	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
87.70.19.170	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 87.70.19.170	Block	9
79.179.164.67	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
64.233.172.162	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
5.28.158.182	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
185.32.179.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
2.52.58.78	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
72.9.148.10	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
132.67.104.164	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
62.219.148.74	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
185.15.104.173	United Kingdom	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
89.138.163.37	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
46.116.27.142	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
64.233.172.178	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
192.55.55.41	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
176.13.16.180	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
77.127.133.132	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
93.173.177.28	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.52	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
87.68.154.122	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6

02-15-2016-16:04:07 to 02-15-2016-17:04:07