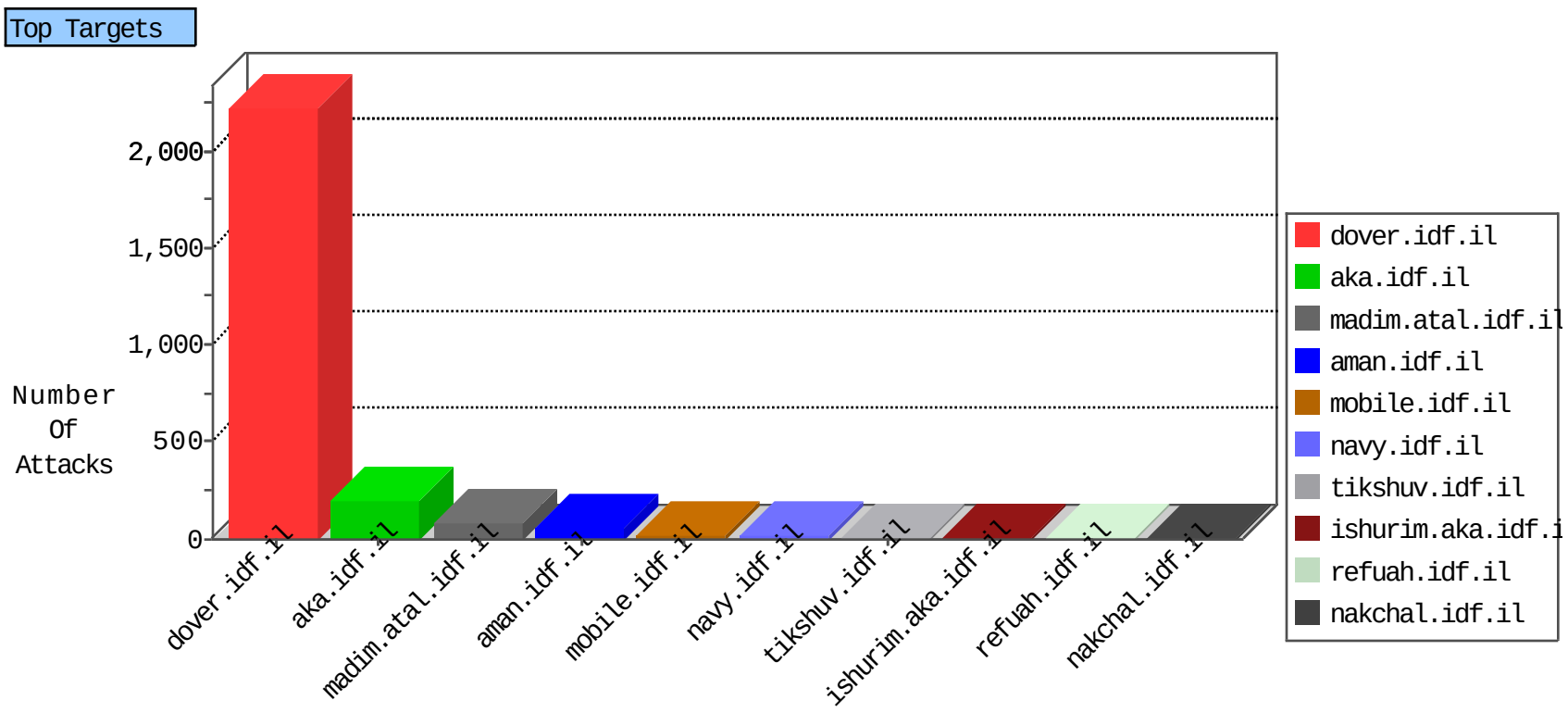
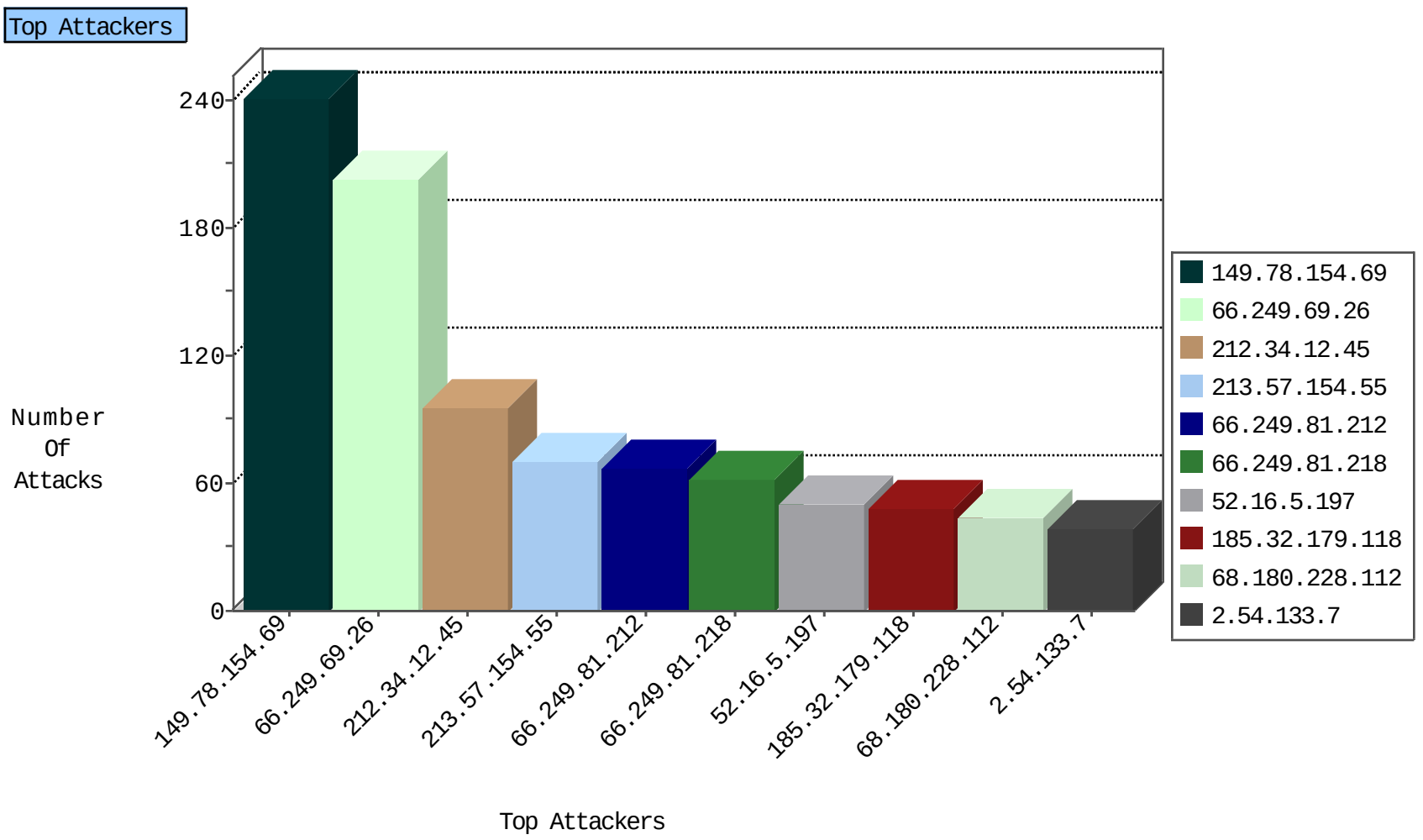
02-13-2016-19:04:05 to 02-13-2016-20:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-13-2016-19:04:05 to 02-13-2016-20:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
89.248.174.4	Netherlands	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
173.252.90.244	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

02-13-2016-19:04:05 to 02-13-2016-20:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.245.64.42	United States	147.237.77.216	dover.idf.il	0543: HTTP: php.cgi Access	Block	1
185.29.240.132	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1
198.245.64.42	United States	147.237.72.166	aka.idf.il	0543: HTTP: php.cgi Access	Block	1
198.245.64.42	United States	147.237.76.86	navy.idf.il	0543: HTTP: php.cgi Access	Block	1

02-13-2016-19:04:05 to 02-13-2016-20:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
93.113.125.11	147.237.77.243	Romania	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.0.15	Turkey	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
37.26.148.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
183.60.48.25	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
182.72.109.162	147.237.76.198	India	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
115.28.218.77	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
93.113.125.11	147.237.77.233	Romania	atal.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.30	China	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.224.178.174	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
98.119.105.221	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1

02-13-2016-19:04:05 to 02-13-2016-20:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.34.12.45	Jordan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
2.54.133.7	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
212.34.12.45	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
109.64.32.138	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.54.133.7	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.133.7	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
62.219.228.23	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.148.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.229.197.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.133.7	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.135.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.211.213.35	Netherlands	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
188.120.148.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.29.49.99	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.34.12.45	Jordan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN 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
5.29.49.99	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.121.92.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
5.102.195.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.154.142.211	Germany	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.177.99.251	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
84.228.50.62	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
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.22.135.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.233	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.66.199.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.13.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.145.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.111.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.120.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.22.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.200.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.17.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.45.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.96.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.37.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.150.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.41.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.175.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.120.125.44		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-13-2016-19:04:05 to 02-13-2016-20:04:05

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
37.46.36.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.158.131	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
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	202
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	67
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	62
213.57.154.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
185.32.179.118	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	48
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	46
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	43
93.172.254.149	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	33
109.66.123.164	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	33
77.126.225.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	32
80.246.137.33	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
109.253.135.137	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
46.19.85.154	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	25
149.78.110.247	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
2.54.53.203	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
149.50.66.165	United States	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	23
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
176.13.17.170	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	21
157.55.39.219	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
46.19.85.4	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
109.65.32.10	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
82.81.15.16	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
109.253.199.121	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
37.26.149.234	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	16
40.77.167.100	United States	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
46.121.218.12	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	14
85.250.228.23	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
5.144.55.180	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
5.29.49.99	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
85.64.122.199	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
213.57.41.149	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
2.54.50.130	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
212.34.12.45	Jordan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 212.34.12.45	Block	10
149.78.221.220	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
83.34.155.134	Spain	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
212.34.12.45	Jordan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 212.34.12.45	Block	10
188.142.188.130	Hungary	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
149.78.128.23	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
85.64.129.48	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
212.34.12.45	Jordan	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 212.34.12.45	Block	8
176.13.16.249	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
213.57.154.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	8
2.54.63.165	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
79.176.176.215	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8

02-13-2016-19:04:05 to 02-13-2016-20:04:05