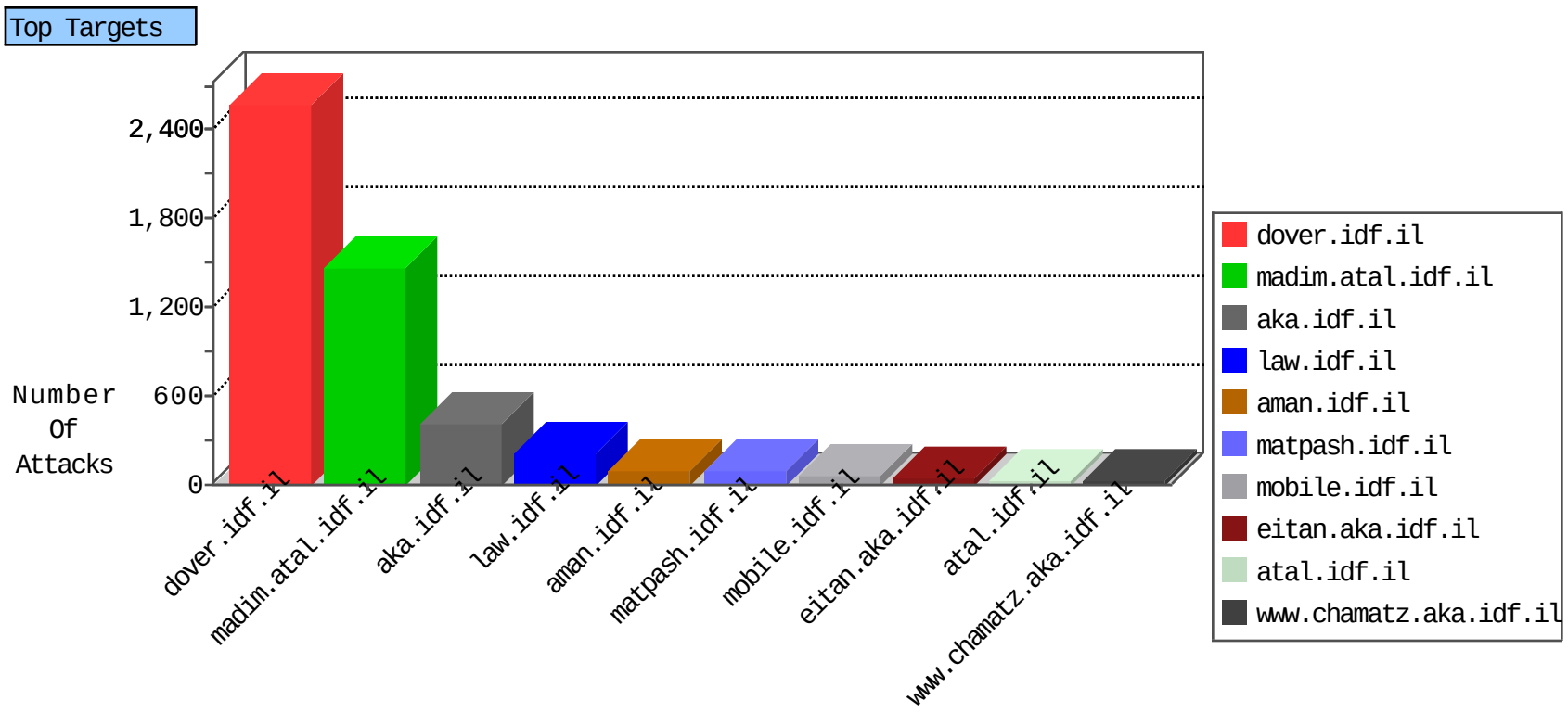
11-28-2015-18:04:07 to 11-28-2015-19:04:07

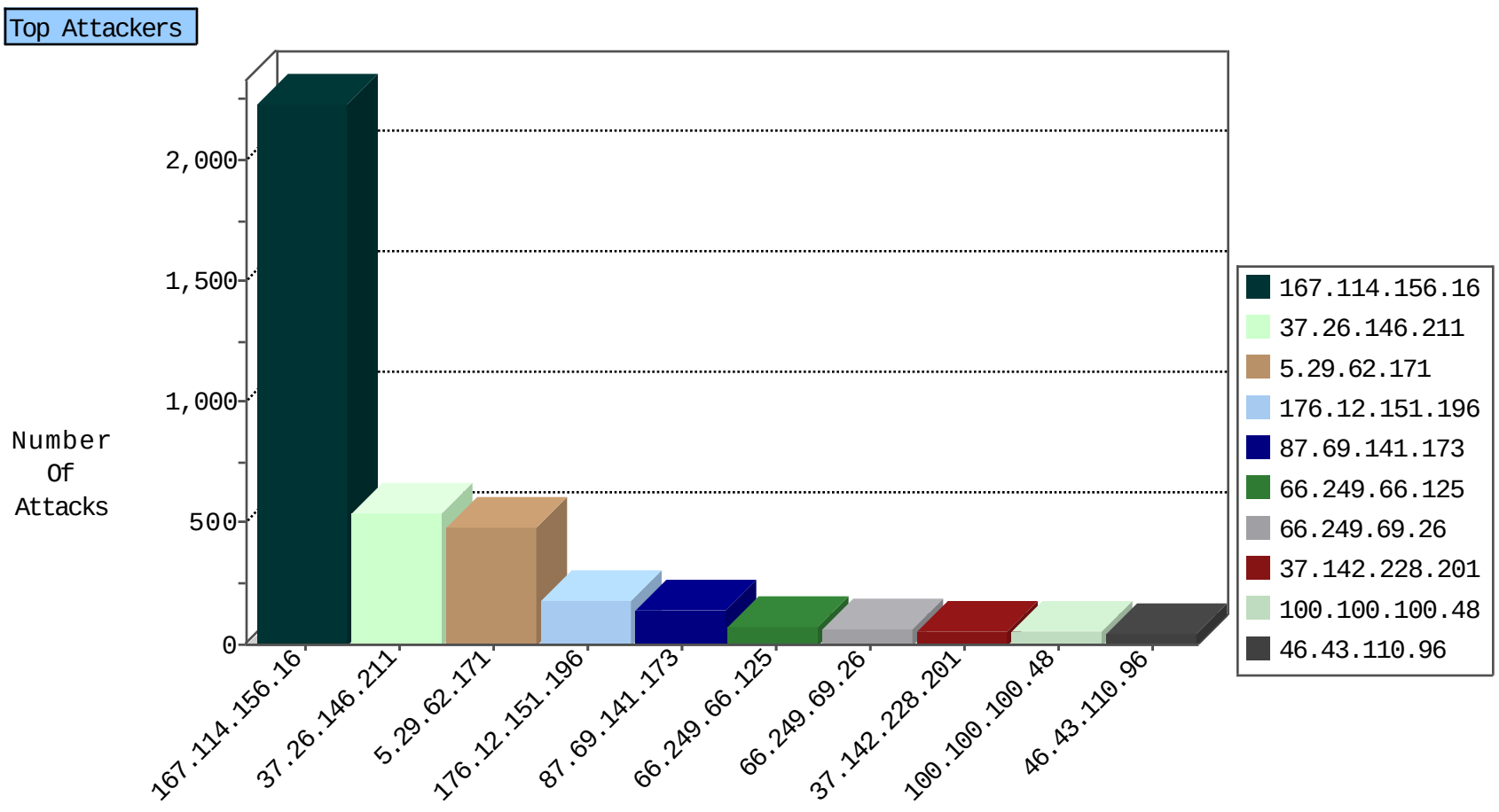
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-28-2015-18:04:07 to 11-28-2015-19:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3516
46.43.110.96	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	2378
66.249.66.39	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	792
54.244.22.103	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	741
66.249.66.33	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	737
66.249.74.97	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	285
79.183.14.170	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
93.174.93.151	Netherlands	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
85.25.43.94	Germany	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

11-28-2015-18:04:07 to 11-28-2015-19:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.154.188.35	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.211.94	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.217.38	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

11-28-2015-18:04:07 to 11-28-2015-19:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.125	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	78
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
54.183.246.95	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
218.104.49.211	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
190.185.208.131	147.237.76.30	Argentina	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
188.214.128.12	147.237.76.199	Romania	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
128.199.139.56	147.237.77.74	Singapore	law.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
115.182.17.13	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN NMAP -f -sS	1
58.253.96.122	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
189.34.74.19	147.237.8.28	Brazil	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
176.12.151.196	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
115.182.17.13	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN NMAP -sS window 2048	1
58.253.96.122	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1

11-28-2015-18:04:07 to 11-28-2015-19:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
79.182.181.144	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
46.43.110.96	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.142.228.201	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	35
100.100.77.54		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	30
100.100.19.155		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
100.100.70.245		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
100.100.11.84		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	24
100.100.76.150		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
100.100.100.48		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
100.100.43.161		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
100.100.39.173		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
213.57.133.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
37.142.228.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
100.100.87.229		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
100.100.100.48		147.237.0.16	my-kosher-kravi.idf.il	drop	First packet isn't SYN	drop	15
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	14
84.228.34.46	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
100.100.100.48		147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	12
40.77.167.35	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.88	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.15.106		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.147.187	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.69.42	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
66.249.93.228	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
100.100.0.69		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	9
79.136.113.86	Sweden	147.237.77.74	law.idf.il	drop	SAM rule	drop	8
100.100.2.84		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.119	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.181	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
109.66.197.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
194.90.167.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.117.154.242	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.188.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.69.34	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.244.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.15.106		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
87.69.210.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.147.180	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.102.136.70	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
177.75.157.37	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
84.108.234.55	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
100.100.17.168		147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	4
5.22.250.240	Netherlands	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
213.205.38.29	Italy	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

11-28-2015-18:04:07 to 11-28-2015-19:04:07

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
77.81.165.43	Romania	147.237.77.74	law.idf.il	drop	SAM rule	drop	4

11-28-2015-18:04:07 to 11-28-2015-19:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	301
5.29.62.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	267
37.26.146.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	129
37.26.146.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	108
5.29.62.171	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 5.29.62.171	Block	107
5.29.62.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
176.12.151.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	91
176.12.151.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	90
87.69.141.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
87.69.141.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
79.179.150.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
185.32.179.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
46.19.86.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
176.13.1.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
176.12.148.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
77.127.202.244	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.127.202.244	Block	5
149.88.123.122	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.88.123.122	Block	5
109.160.204.186	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	4
87.230.85.14	Germany	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
216.172.176.112	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
37.26.148.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.172.174.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.56.62.44	United Kingdom	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
146.185.149.117	Netherlands	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
213.205.38.29	Italy	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
50.87.107.49	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
162.242.152.71	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
66.147.240.155	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
50.87.52.71	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
162.144.123.182	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
200.73.17.115	Chile	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
37.26.147.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
193.180.217.93	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
185.41.10.58	United Kingdom	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
192.163.238.217	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
212.48.87.37	United Kingdom	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	3
79.182.214.85	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
176.56.62.44	United Kingdom	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	2
50.87.52.71	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
146.185.149.117	Netherlands	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	2
185.41.10.58	United Kingdom	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 185.41.10.58	Block	2
213.205.38.29	Italy	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	2
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
200.73.17.115	Chile	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/index.php	Block	2
50.87.107.49	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
162.242.152.71	United States	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	2
66.147.240.155	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	2
50.87.52.71	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	2
192.163.238.217	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/index.php	Block	2
162.144.123.182	United States	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	2

11-28-2015-18:04:07 to 11-28-2015-19:04:07