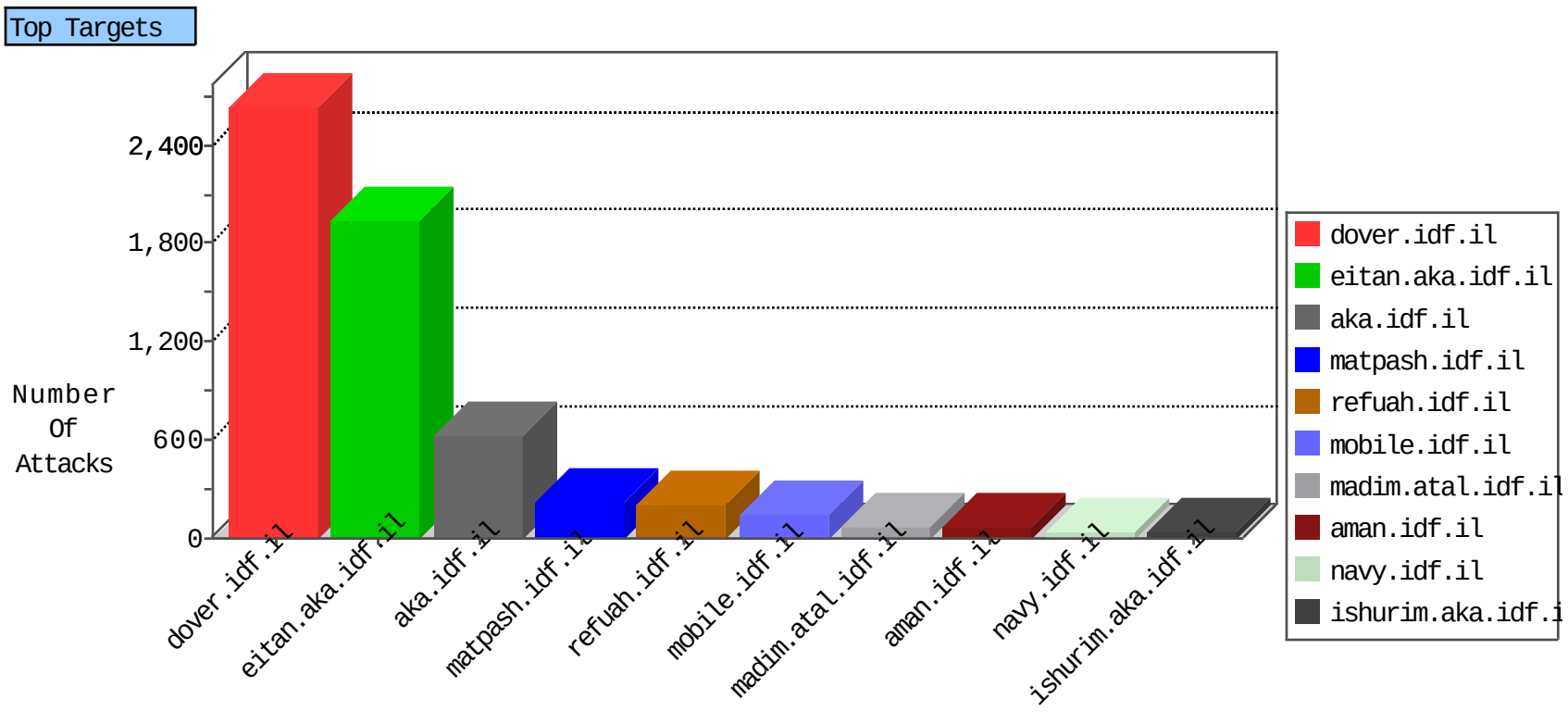
11-30-2015-11:04:03 to 11-30-2015-12:04:03

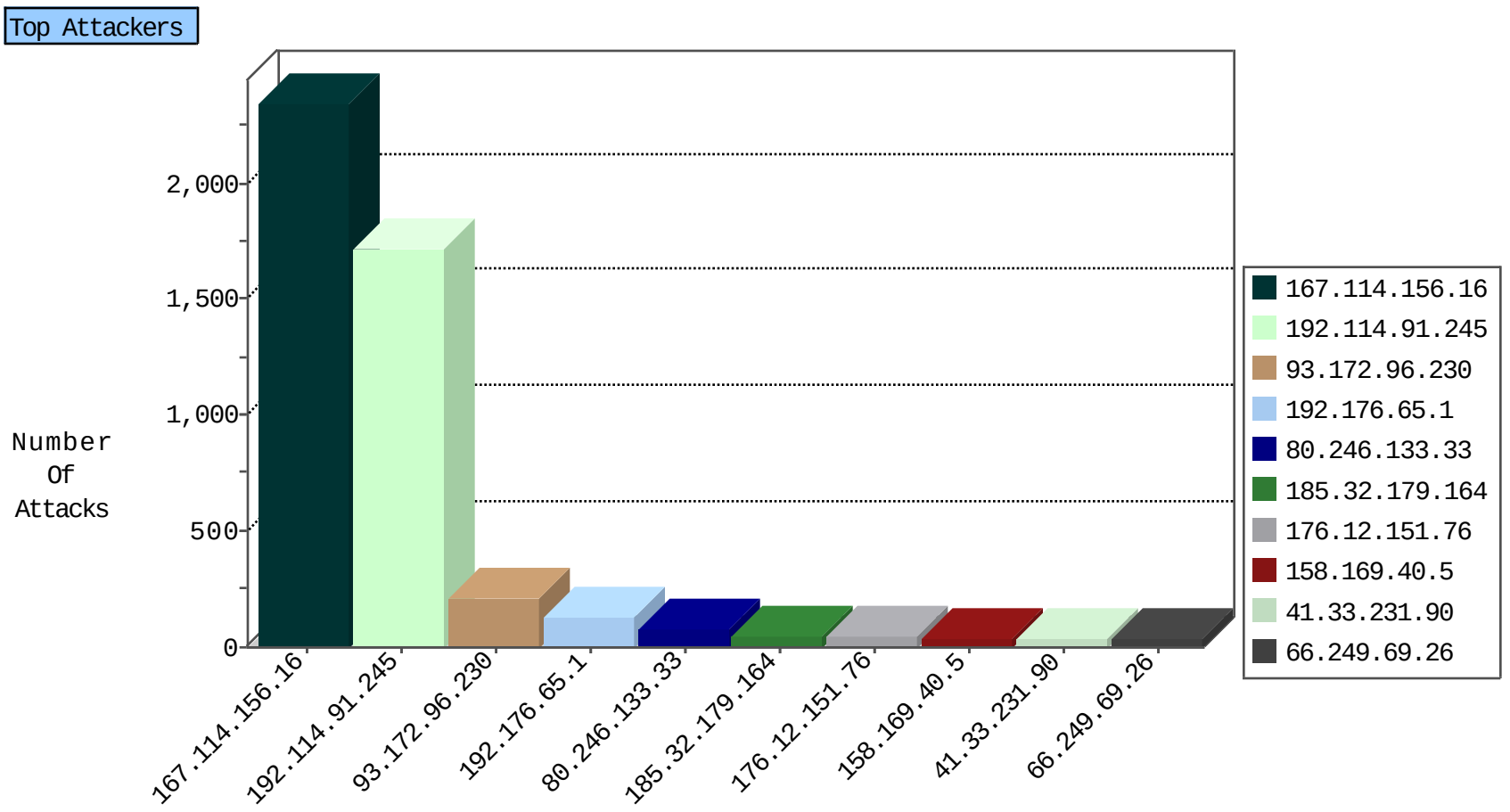
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-30-2015-11:04:03 to 11-30-2015-12:04:03

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	3240
66.249.66.61	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	151
222.186.34.238	China	147.237.0.35	akaws.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
93.174.93.151	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.220	Switzerland	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
93.174.93.151	Netherlands	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
216.119.7.56	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
218.104.198.195	China	147.237.76.202	e.halag.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
93.174.93.151	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.169	Switzerland	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1

11-30-2015-11:04:03 to 11-30-2015-12:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.90.66.15	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
212.25.95.14	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
195.154.217.216	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.188.35	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.194.58	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

11-30-2015-11:04:03 to 11-30-2015-12:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.81.198	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
81.218.206.48	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.242	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	147.237.77.227	Cote D'Ivoire	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
176.13.4.88	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
87.68.157.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.1.60	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.213.132.147	147.237.72.166	China	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.175.232	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.154.188.35	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
158.169.40.6	147.237.77.216	Belgium	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1

11-30-2015-11:04:03 to 11-30-2015-12:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.114.91.245	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	1371
192.176.65.1	Sweden	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	130
80.246.133.33	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	75
176.12.151.76	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
158.169.40.5	Belgium	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
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
100.100.53.201		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
31.168.2.130	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
2.54.174.101	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
80.246.130.130	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
93.172.96.230	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.52.164.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.157.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
137.95.1.11	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	14
2.54.19.149	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
192.118.78.198	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	12
176.12.139.234	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.118.78.198	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
100.100.120.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
100.100.120.33		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
195.160.240.11	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
2.52.133.212	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.52.189.67	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
84.228.194.62	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.118.78.57	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
213.57.142.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
213.57.142.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.86.18	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
213.57.137.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
58.11.36.47	Thailand	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
185.32.179.229	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
2.52.130.67	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
192.116.127.113	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
100.100.108.213		147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	7
212.199.244.112	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
213.57.137.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
2.54.11.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.135.251	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
192.114.91.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.155.137	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.183.169.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.159	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.54.11.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	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
46.19.85.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.81.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.130.223.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

11-30-2015-11:04:03 to 11-30-2015-12:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.114.91.245	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	345
93.172.96.230	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	191
46.19.86.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
185.32.179.164	Israel	147.237.77.243	mobile.idf.il	System32 Access	Block	15
185.32.179.164	Israel	147.237.77.243	mobile.idf.il	Multiple System32 access(+) from 185.32.179.164	Block	14
176.12.142.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
185.32.179.164	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	12
46.19.86.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
176.12.147.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
46.19.86.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/$$$&?&?$$$	Block	6
46.19.85.128	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	6
176.12.149.190	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	6
2.52.164.32	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
95.134.121.18	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	5
2.52.164.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
79.182.217.102	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
24.213.216.70	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
187.32.58.200	Brazil	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
176.13.17.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.48.87.37	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
186.202.161.36	Brazil	147.237.76.86	navy.idf.il	PHP Attempt	Block	3
27.50.81.250	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
68.171.222.114	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
108.175.150.166	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
173.247.248.14	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	3
77.74.51.87	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
173.247.248.14	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/index.php	Block	2
187.32.58.200	Brazil	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
212.48.87.37	United Kingdom	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
27.50.81.250	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
68.171.222.114	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
46.19.86.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
108.175.150.166	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
24.213.216.70	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/index.php	Block	2
77.74.51.87	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
46.120.116.64	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
37.26.149.246	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
27.50.81.250	Australia	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
109.66.31.206	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
68.171.222.114	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
108.175.150.166	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
77.74.51.87	Netherlands	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
187.32.58.200	Brazil	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
212.48.87.37	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	2
186.202.161.36	Brazil	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/index.php	Block	2
91.213.233.164	Kyrgyzstan	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
46.19.86.177	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
108.175.150.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 108.175.150.166	Block	1

11-30-2015-11:04:03 to 11-30-2015-12:04:03