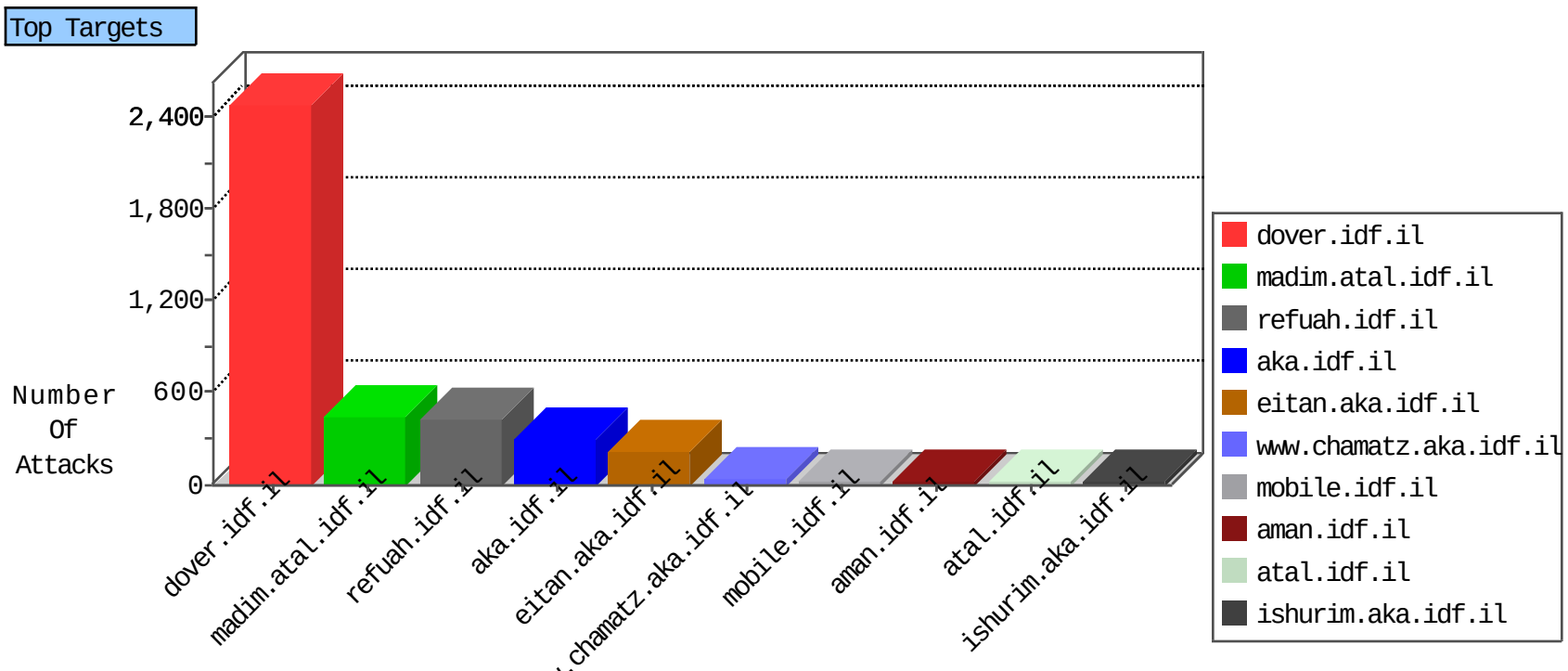
12-17-2015-14:04:03 to 12-17-2015-15:04:03

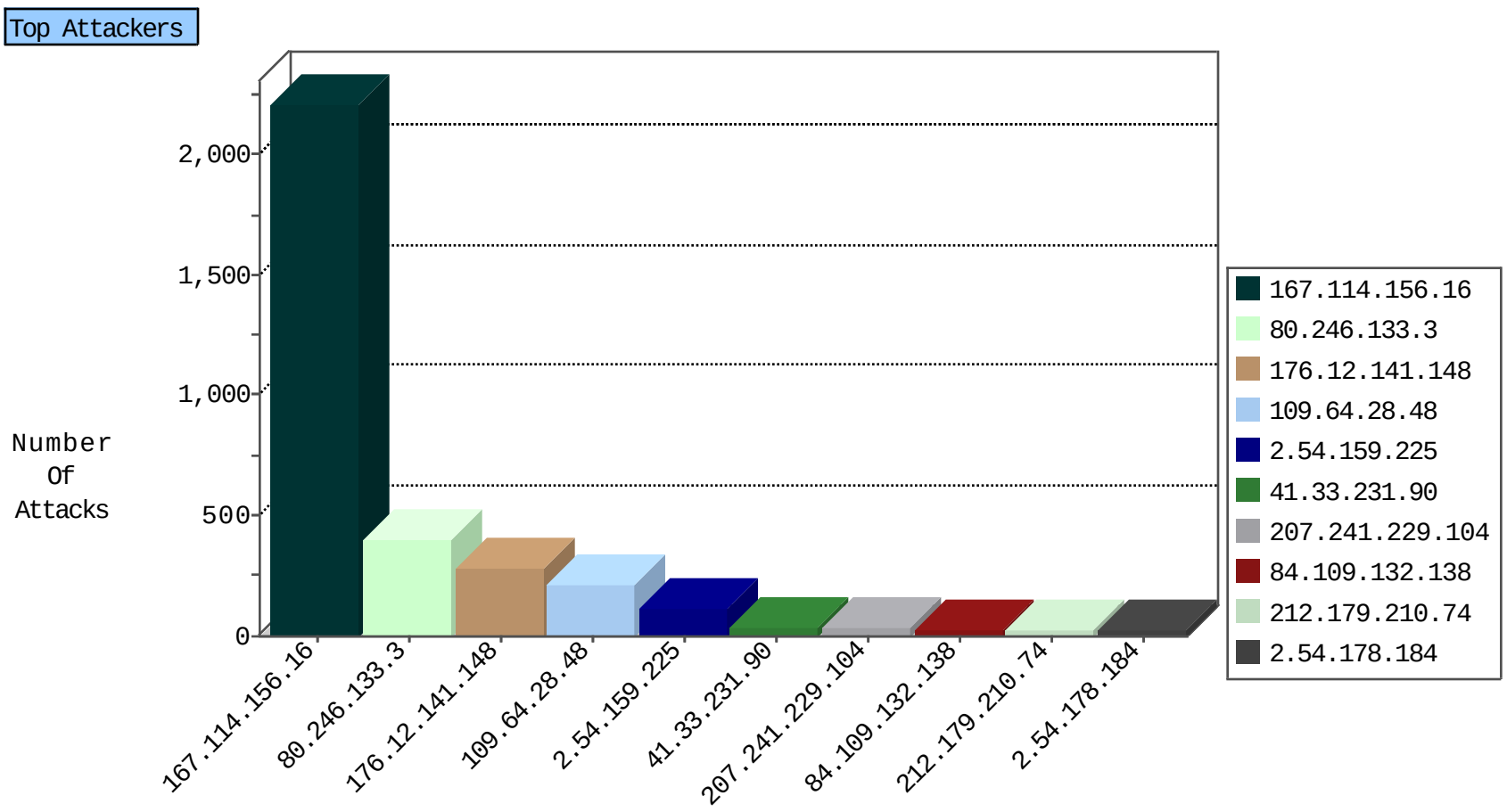
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

12-17-2015-14:04:03 to 12-17-2015-15:04:03

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	3559
66.249.64.55	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	332

12-17-2015-14:04:03 to 12-17-2015-15:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.79	France	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
46.105.17.34	France	147.237.77.170	maarachot.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-17-2015-14:04:03 to 12-17-2015-15:04:03

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	2
146.185.250.2	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN NMAP -sS window 1024	1
122.4.237.235	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
122.4.237.235	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
122.4.237.235	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
87.69.245.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.221.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.248	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.140	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.5.140	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
146.185.250.2	147.237.76.39	Russian Federation	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
122.4.237.235	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
122.4.237.235	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
93.173.164.234	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.249.175.230	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
84.228.202.243	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.76.100.12	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.139.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.149.159	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.168.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

12-17-2015-14:04:03 to 12-17-2015-15:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
80.246.133.3	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	402
109.64.28.48	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	204
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
207.241.229.104	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
80.179.114.19	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	17
207.241.229.104	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	13
172.58.169.112	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
81.218.174.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
212.179.210.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
212.179.210.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
31.13.112.122	Ireland	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.56	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
213.57.141.124	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.162	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.178.184	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.171	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
31.13.109.121	Ireland	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
109.162.164.102	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.127.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.167	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.150.66.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
132.66.223.8	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.68.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.183.229.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.68.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.162.164.102	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.56	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
2.54.178.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
149.88.5.152	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.171	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
207.46.13.81	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
31.13.112.118	Ireland	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	5
2.54.178.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.109.3.6	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.57.135.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.160	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.80.30.90	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
31.13.112.123	Ireland	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
82.80.30.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
62.0.230.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
89.138.251.105	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.136.185	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.25.117	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.90	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.177.200.234	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

12-17-2015-14:04:03 to 12-17-2015-15:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.141.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	118
176.12.141.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	100
2.54.159.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
176.12.141.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	67
84.109.132.138	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.109.132.138	Block	26
2.54.159.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	21
176.13.16.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
176.13.23.217	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	7
2.54.22.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.12.140.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.12.139.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.54.24.90	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22354-he/dover	Block	4
2.54.142.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
82.80.216.12	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/120203	Block	3
84.110.211.46	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22354-he/dover	Block	3
46.19.85.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.143.73	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
81.218.35.242	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
5.28.181.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22354-he/dover	Block	2
37.26.149.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
176.13.18.150	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22354-he/dover	Block	2
2.54.42.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
85.250.173.111	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22354-he/dover	Block	2
46.19.86.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.111.184.168	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/xmlrpc.php	Block	1
80.246.139.163	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
216.218.206.68	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
5.28.137.100	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
157.55.39.13	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
77.127.152.56	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
207.46.13.128	United States	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
184.105.139.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
87.208.0.108	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
37.26.149.237	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22354-he/dover	Block	1
79.183.229.161	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.179.210.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
195.60.232.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.59.155.109	United Arab Emirates	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
85.64.92.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.13	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/w/load.php	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.176.97.218	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.128	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/administrator/minipres_manager/get_booking_minipre_responsive	Block	1
46.19.86.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-17-2015-14:04:03 to 12-17-2015-15:04:03