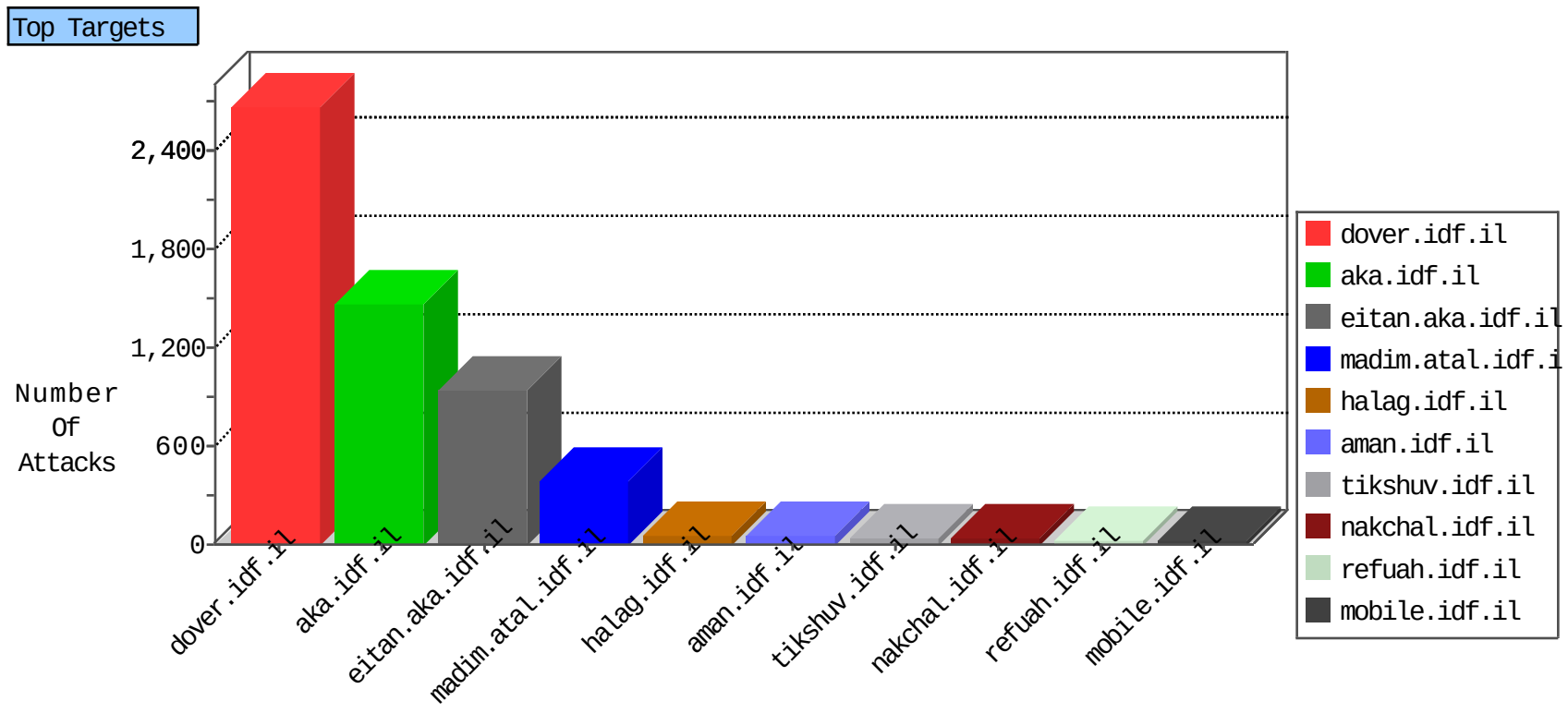
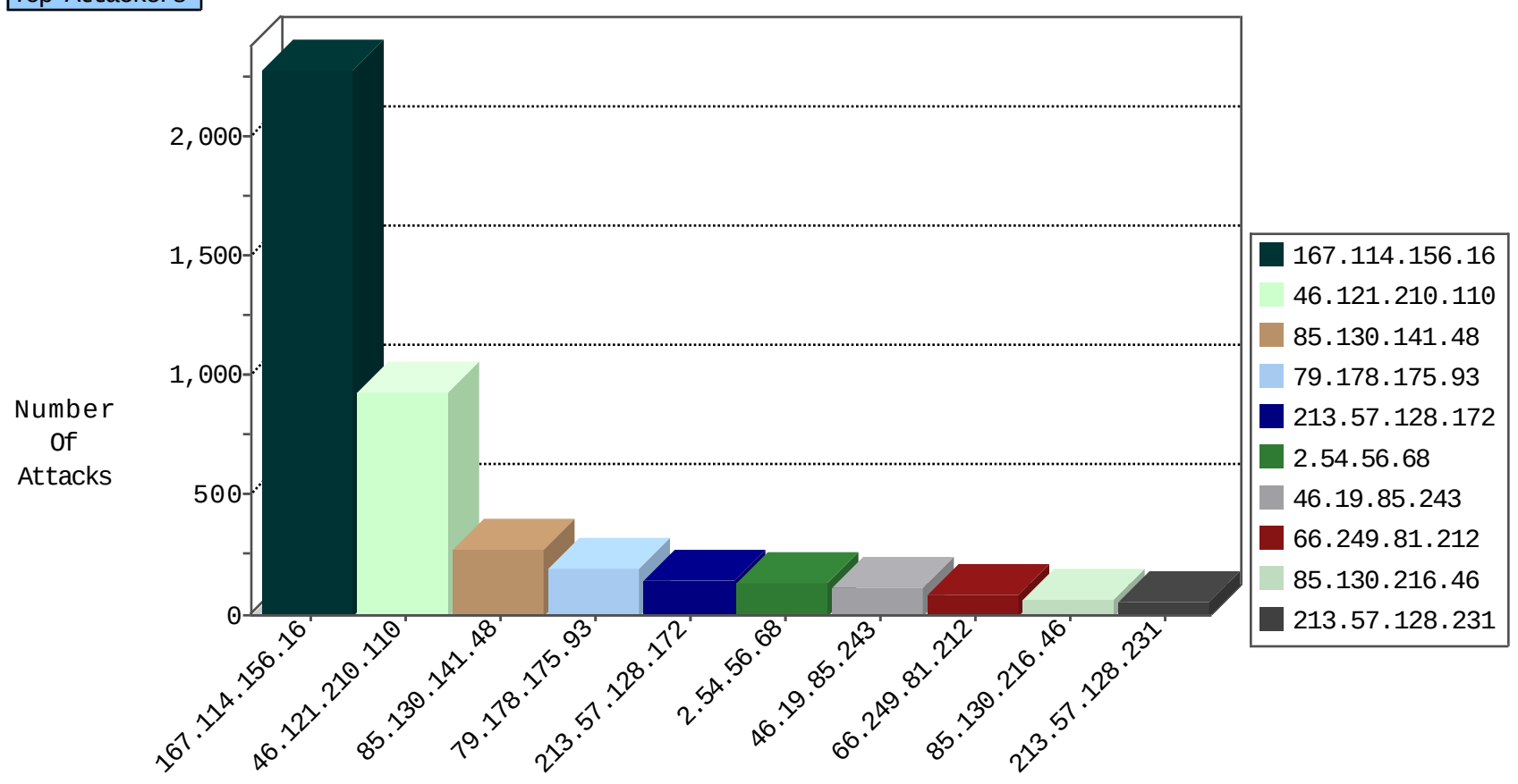
11-26-2015-21:04:05 to 11-26-2015-22:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-26-2015-21:04:05 to 11-26-2015-22:04:05

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	3766
71.232.12.208	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	452
66.249.66.78	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	383
178.204.101.17	Russian Federation	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	2
120.155.132.3	Australia	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

11-26-2015-21:04:05 to 11-26-2015-22:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.243.60	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
185.120.125.9		147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
93.172.162.134	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
188.165.15.196	France	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-26-2015-21:04:05 to 11-26-2015-22:04:05

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	4
66.249.75.106	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
162.222.185.165	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
149.88.78.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
119.73.228.130	147.237.76.176	Singapore	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.76.31	Turkey	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
216.251.24.119	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
46.172.71.252	147.237.8.28	Ukraine	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
162.222.185.165	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
119.73.228.130	147.237.76.176	Singapore	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
93.113.125.11	147.237.76.30	Romania	himush.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.227.85	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
216.251.24.119	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
162.222.185.165	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
162.222.185.165	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1

11-26-2015-21:04:05 to 11-26-2015-22:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.121.210.110	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	783
85.130.141.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	139
85.130.141.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	138
213.57.128.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	136
2.54.56.68	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	104
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	82
213.57.128.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	57
79.182.181.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.86.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
188.120.148.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
213.57.130.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
100.100.32.249		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
80.246.130.95	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
66.249.81.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
100.100.124.9		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
85.130.216.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
100.100.126.8		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
217.132.8.196	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
100.100.106.25		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	20
89.72.136.2	Poland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
100.100.29.63		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
100.100.62.70		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
100.100.9.206		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
37.142.237.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
100.100.112.61		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
85.130.216.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.85.156	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
85.130.216.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
100.100.19.209		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
85.130.222.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.74.64		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
188.120.148.154	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.216.46	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
100.100.119.105		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
87.69.194.9	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
213.57.139.162	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
213.57.151.207	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
109.64.4.192	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
80.246.137.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.160.141.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.85.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.56.68	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
46.19.85.156	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	8
100.100.119.105		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
2.54.56.68	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.56.68	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
85.250.220.136	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7

11-26-2015-21:04:05 to 11-26-2015-22:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.175.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	164
46.121.210.110	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 46.121.210.110	Block	153
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	105
85.65.33.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
79.178.175.93	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.178.175.93	Block	25
93.172.37.225	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 93.172.37.225	Block	20
109.66.210.109	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.66.210.109	Block	17
176.13.21.187	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	8
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
109.186.153.11	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	7
46.19.85.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	6
84.109.106.12	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
77.127.214.146	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	5
79.180.222.196	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	4
109.64.4.192	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/7/size338x0/1877.jpg	Block	3
188.120.148.154	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
213.57.175.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.65.33.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	3
2.54.133.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
188.120.148.158	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
31.168.184.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
46.19.85.51	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	2
82.166.140.117	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/1133-22638-he/dover.aspx.	Block	2
46.19.86.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.182.169.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.57.184.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	1
104.192.0.226	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to /js/general.js	Block	1
40.77.167.35	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1560-en/dover.aspx"	Block	1
84.109.65.3	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
207.46.13.113	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
65.203.132.29	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
93.172.37.225	Israel	147.237.72.166	aka.idf.il	Unknown Parameter c in www.aka.idf.il/main/haredim/general.aspx	None	1
31.210.187.202	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
79.191.18.28	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	1
157.55.39.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19116-en/dover.aspxhaz	Block	1
79.178.175.93	Israel	147.237.0.19	madim.atal.idf.i	SSL Untraceable Connection - Open Mode	None	1
109.67.186.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.117.174.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.69.32.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.38.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1133-he/dover.aspx	Block	1
46.19.85.218	Israel	147.237.76.30	himush.idf.il	Malformed URL	Block	1
31.210.189.252	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1

11-26-2015-21:04:05 to 11-26-2015-22:04:05