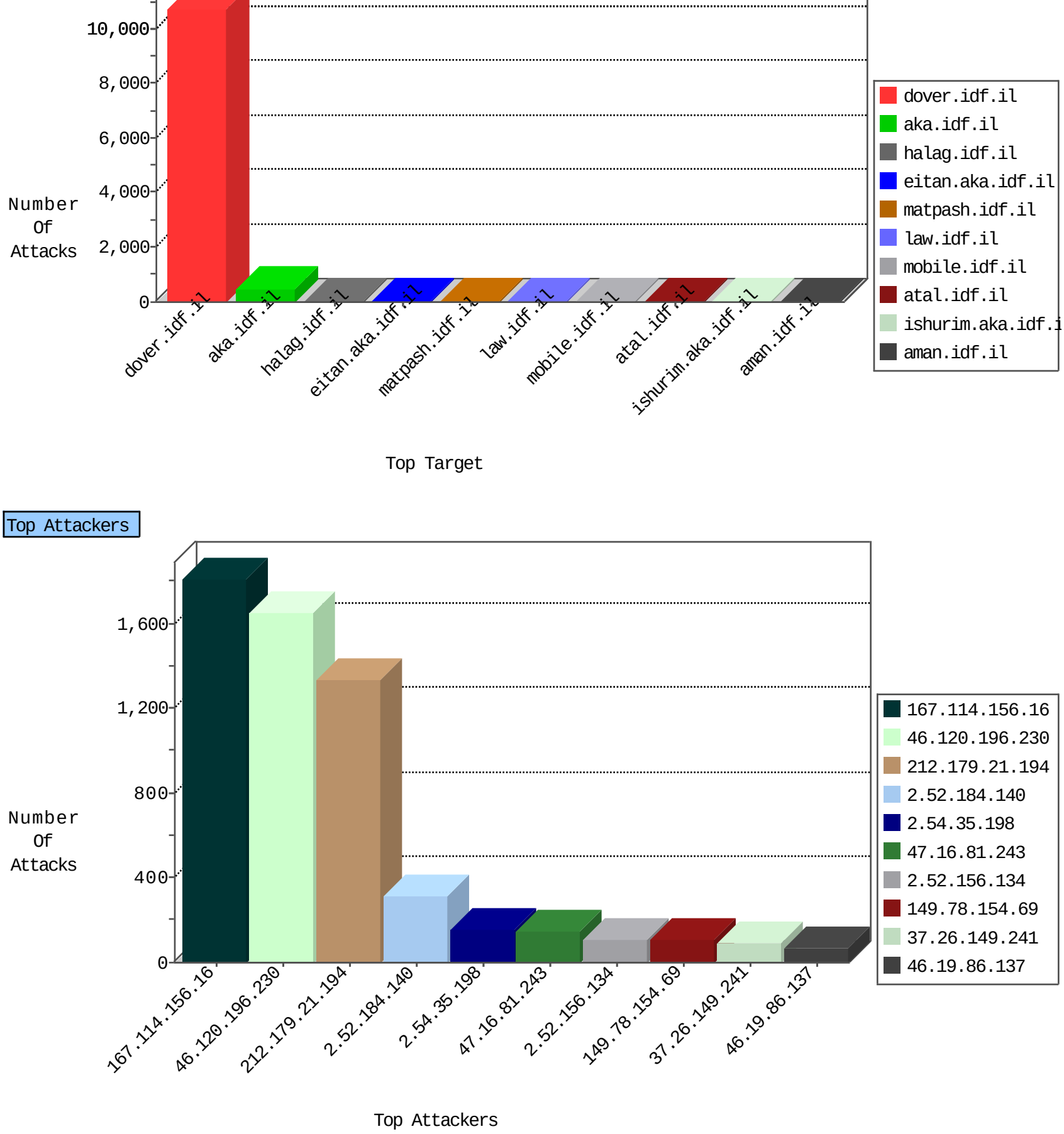
11-03-2015-17:04:06 to 11-03-2015-18:04:06

IDF Under Attack Daily Report



11-03-2015-17:04:06 to 11-03-2015-18:04:06

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	TCP handshake violation, first packet not syn	drop	5496
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2787
66.249.67.79	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1670
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1194
167.220.196.128	United Kingdom	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	1142
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	989
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	917
41.42.147.82	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	885
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	824
132.162.117.239	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	601
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	534
66.249.79.43	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	516
66.249.79.45	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	490
66.249.79.41	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	411
66.249.69.42	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	316
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	183
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	157
67.68.24.94	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	150
146.185.56.162	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	32
79.180.168.47	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
66.249.83.158	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	22
185.24.207.16	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
2.54.129.32	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	17
23.242.215.155	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	17
46.117.242.238	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
5.29.71.133	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
80.246.137.253	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
79.177.201.90	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
93.47.249.99	Italy	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
5.22.129.212	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
84.229.132.151	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
104.162.163.237	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
47.16.81.243	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
37.142.236.249	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
37.142.128.154	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
2.54.178.227	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
85.130.209.137	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
2.54.148.35	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
93.172.183.208	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
176.12.148.253	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
46.31.103.60	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
95.86.127.113	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
81.218.141.87	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
62.90.203.34	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.181.207.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
132.162.117.239	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
213.151.37.96	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.7.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
31.168.218.33	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4

11-03-2015-17:04:06 to 11-03-2015-18:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
202.134.8.135	Bangladesh	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	6
5.29.147.113	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-03-2015-17:04:06 to 11-03-2015-18:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.83.254	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	5
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	3
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.79.43	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
37.26.149.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.138.9.51	147.237.77.234	Germany	halag.idf.il	ET SCAN NMAP -sS window 1024	1
113.59.33.61	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
109.66.200.201	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.243	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.64.91	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
188.138.9.51	147.237.0.16	Germany	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
132.162.117.239	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
112.216.109.98	147.237.72.167	Korea, Republic of	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
95.156.251.10	147.237.77.176	Germany	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
46.118.155.220	147.237.77.216	Ukraine	dover.idf.il	portscan: TCP Distributed Portscan	1

11-03-2015-17:04:06 to 11-03-2015-18:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.120.196.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1652
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1302
2.52.184.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	313
2.54.35.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	147
47.16.81.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	138
2.52.156.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	109
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
37.26.149.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	92
46.19.86.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
46.19.85.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
37.26.148.186	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
46.19.85.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
31.154.173.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
207.46.13.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
66.249.83.171	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
66.249.83.161	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
80.178.157.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
87.69.248.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
212.14.228.122	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
2.54.128.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
23.242.215.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
100.100.17.169		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	35
100.100.6.67		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	34
84.94.91.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
109.160.141.94	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
109.67.165.127	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
46.19.86.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
149.88.224.77	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
66.249.69.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
146.185.56.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
176.13.6.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
46.19.86.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
77.125.84.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
93.47.249.99	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.19.85.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
62.57.73.244	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
5.29.5.124	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
37.142.128.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
85.64.89.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
37.142.64.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.85.30	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.85.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
176.12.148.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
2.54.7.199	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24

11-03-2015-17:04:06 to 11-03-2015-18:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.112	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	9
213.57.170.195	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	5
213.57.170.195	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	5
213.57.170.195	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	5
84.95.48.97	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
84.95.48.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	4
84.95.48.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
79.178.178.149	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	4
79.177.205.43	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	3
66.249.65.53	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
176.13.22.144	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
37.26.147.199	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/	Block	2
79.182.206.46	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.54.39.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.182.124.135	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	2
79.182.124.135	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/ajax/updatestatus.php	Block	2
31.154.91.114	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
93.173.29.3	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/ajax/updatestatus.php	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.228.164.80	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	1
46.19.85.195	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
79.182.181.161	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.182.181.161	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9692-he/refuah.aspx	Block	1
31.154.92.223	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
109.186.156.95	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
2.52.152.77	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
87.69.87.158	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/960.css	Block	1
46.229.164.98	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper	Block	1
37.142.103.176	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/1682.doc"	Block	1
149.88.85.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	1
79.179.137.105	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.154.91.114	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	1
109.64.172.57	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.65.55	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2418.jpg	Block	1
217.194.199.151	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
84.228.164.80	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
79.182.181.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
46.19.85.195	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version _pk_id.20.8afc=e6403868357c7aff.1423772643.5.1446563829.1446563829.; _pk_ses.20.8afc=*	Block	1
176.106.227.186	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1111-he/nakhal.aspx	Block	1
141.212.121.208	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 147.237.0.34/	Block	1
2.54.10.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.69.245.180	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.67.41	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.65.34	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/2616.jpg	Block	1
40.77.167.98	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
149.88.85.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1

11-03-2015-17:04:06 to 11-03-2015-18:04:06