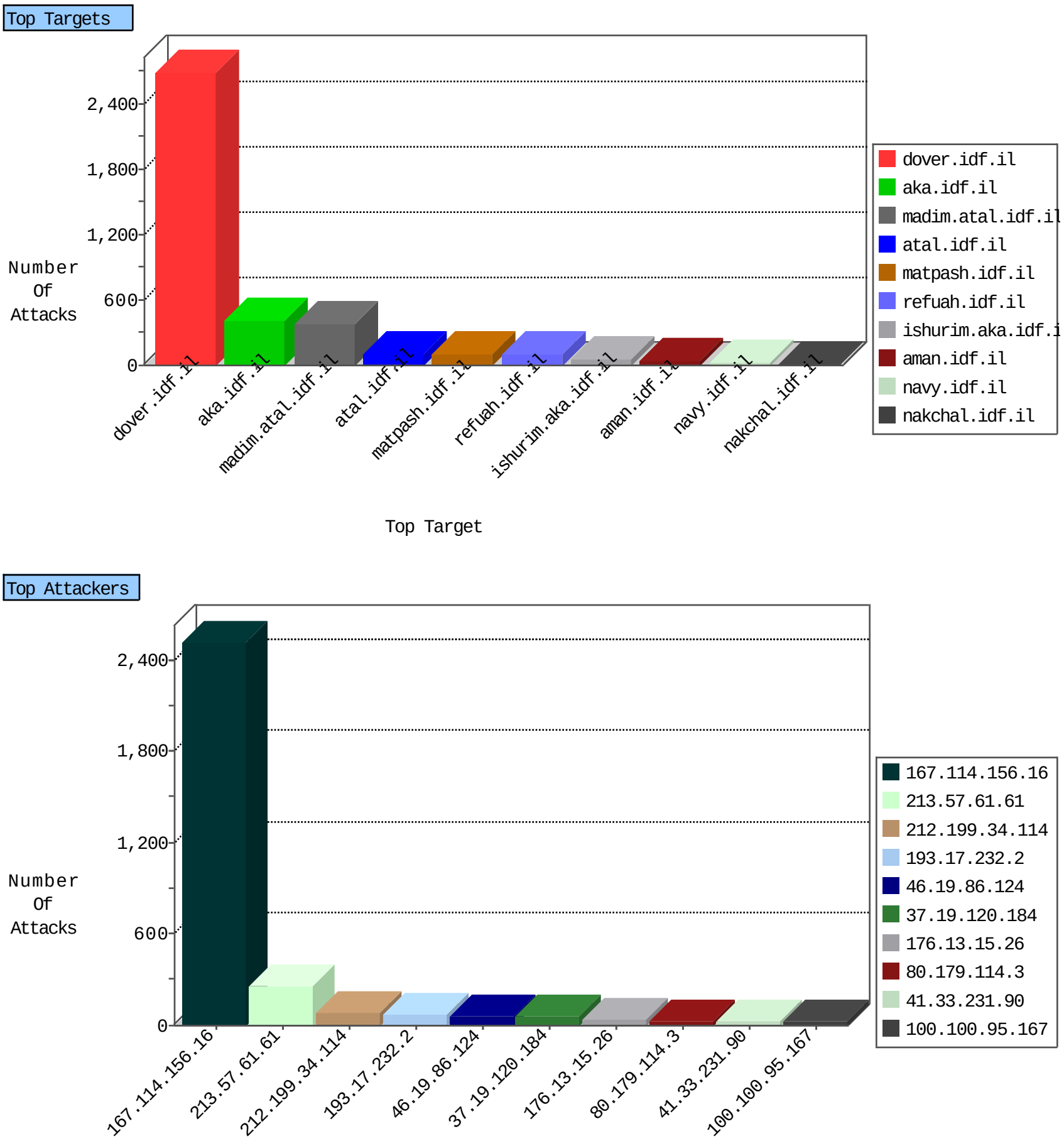
12-03-2015-12:04:03 to 12-03-2015-13:04:03

IDF Under Attack
Daily Report



12-03-2015-12:04:03 to 12-03-2015-13:04:03

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	3340
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
147.236.238.250	Israel	147.237.0.15	kosher-kravi.idf.il	Block_Udp_All_Nets	drop	3
147.236.238.250	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
180.97.106.162	China	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
180.97.106.36	China	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
115.239.228.8	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Http	drop	1
180.97.106.161	China	147.237.0.19	madim.atal.idf.il	block-sp-traf1	drop	1
180.97.106.162	China	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
180.97.106.36	China	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
146.185.239.100	Russian Federation	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
180.97.106.161	China	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	drop	1
180.97.106.36	China	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	drop	1
180.97.106.162	China	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
180.97.106.37	China	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
180.97.106.161	China	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1
180.97.106.36	China	147.237.0.34	tikshuv.idf.il	block-sp-traf1	drop	1
110.143.66.246	Australia	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
192.3.170.124	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.37	China	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1

12-03-2015-12:04:03 to 12-03-2015-13:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
69.30.215.142	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
105.103.248.100	Algeria	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	1

12-03-2015-12:04:03 to 12-03-2015-13:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
105.103.248.100	147.237.77.216	Algeria	dover.idf.il	SQL Injection - Select From	2
176.12.140.83	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
105.156.32.56	147.237.77.216	Morocco	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.86.203	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.29.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.0.99.250	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.38.9	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
177.124.125.217	147.237.76.201	Brazil	e.atal.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.255	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
177.124.125.217	147.237.72.167	Brazil	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
37.26.147.219	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
177.124.125.217	147.237.72.156	Brazil	aman.idf.il	ET SCAN Potential SSH Scan	1
177.124.125.217	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Potential SSH Scan	1
177.124.125.217	147.237.0.15	Brazil	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
146.185.56.190	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
84.108.24.107	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.112.102.211	147.237.0.34		tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
177.124.125.217	147.237.76.39	Brazil	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
37.26.148.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
177.124.125.217	147.237.72.166	Brazil	aka.idf.il	ET SCAN Potential SSH Scan	1
177.124.125.217	147.237.72.14	Brazil	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
177.124.125.217	147.237.0.33	Brazil	idf.il	ET SCAN Potential SSH Scan	1

12-03-2015-12:04:03 to 12-03-2015-13:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.199.34.114	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	78
193.17.232.2	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	70
37.19.120.184	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	55
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
213.57.61.61	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
100.100.95.167		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
100.100.32.98		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
80.179.114.3	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
80.179.114.3	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
188.120.148.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.171	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
100.100.94.78		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.21	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	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
147.236.238.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	8
46.19.85.251	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
62.128.48.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
80.179.206.93	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	7
79.181.53.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.128.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.176.154.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.128.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.54.28.29	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.25.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.102.254.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.154.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.213.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.21	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.120.136.211	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.128.48.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
141.0.13.117	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
183.13.127.224	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
80.246.137.147	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
188.120.148.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
188.120.148.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.179.206.93	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
157.55.12.71	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
62.128.48.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
2.52.162.9	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.193	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.177.164.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.53.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.128.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-03-2015-12:04:03 to 12-03-2015-13:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.61.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	127
213.57.61.61	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 213.57.61.61	Block	99
46.19.86.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
176.13.15.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
109.186.16.246	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/ufi/reaction/	Block	7
79.183.219.181	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	7
79.176.122.228	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storage/files/8/	Block	6
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
105.103.248.100	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.103.248.100	Block	4
83.244.36.154	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	3
192.116.55.253	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	3
79.176.122.228	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	3
2.54.171.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
188.161.106.204	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	2
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
176.12.140.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.179.132.201	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	2
176.13.12.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.250.195.148	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	2
80.246.136.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
128.74.205.171	Russian Federation	147.237.0.19	madim.atal.idf.il	Parameter Type Violation returnurl in madim.atal.idf.il/login.aspx	Block	1
77.125.141.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.119	Israel	147.237.77.74	law.idf.il	Distributed Abnormally Long Request	Block	1
105.103.248.100	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/abc123/	Block	1
37.26.146.175	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
87.69.190.81	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.13.13.183	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.88.153.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.60.105	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.151.43.108	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0ahukewjjxasgvl_jahukcrqkhuaob0mqfggimaa&usg=afqjcnhcvyyg7w1cq-yhd5_ammzoyodtwa	Block	1
46.116.219.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.164	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.183.186.96	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.64	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71854-he/maarachot.aspx	Block	1
183.13.127.224	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
41.131.100.197	Egypt	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php	Block	1
95.86.123.214	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0ahukewjljvc_ur_jahxjwrqkhcunc4kqfggumae&usg=afqjcnhcvyyg7w1cq-yhd5_ammzoyodtwa	Block	1
46.121.78.64	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
176.13.2.154	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.190.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.195.148	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/login.aspx	None	1
80.246.137.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
128.232.110.29	United Kingdom	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	1
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	1
78.128.92.193	Bulgaria	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
46.19.85.119	Israel	147.237.77.74	law.idf.il	Illegal HTTP Version _pk_ses.115.5e0a=*	Block	1

12-03-2015-12:04:03 to 12-03-2015-13:04:03