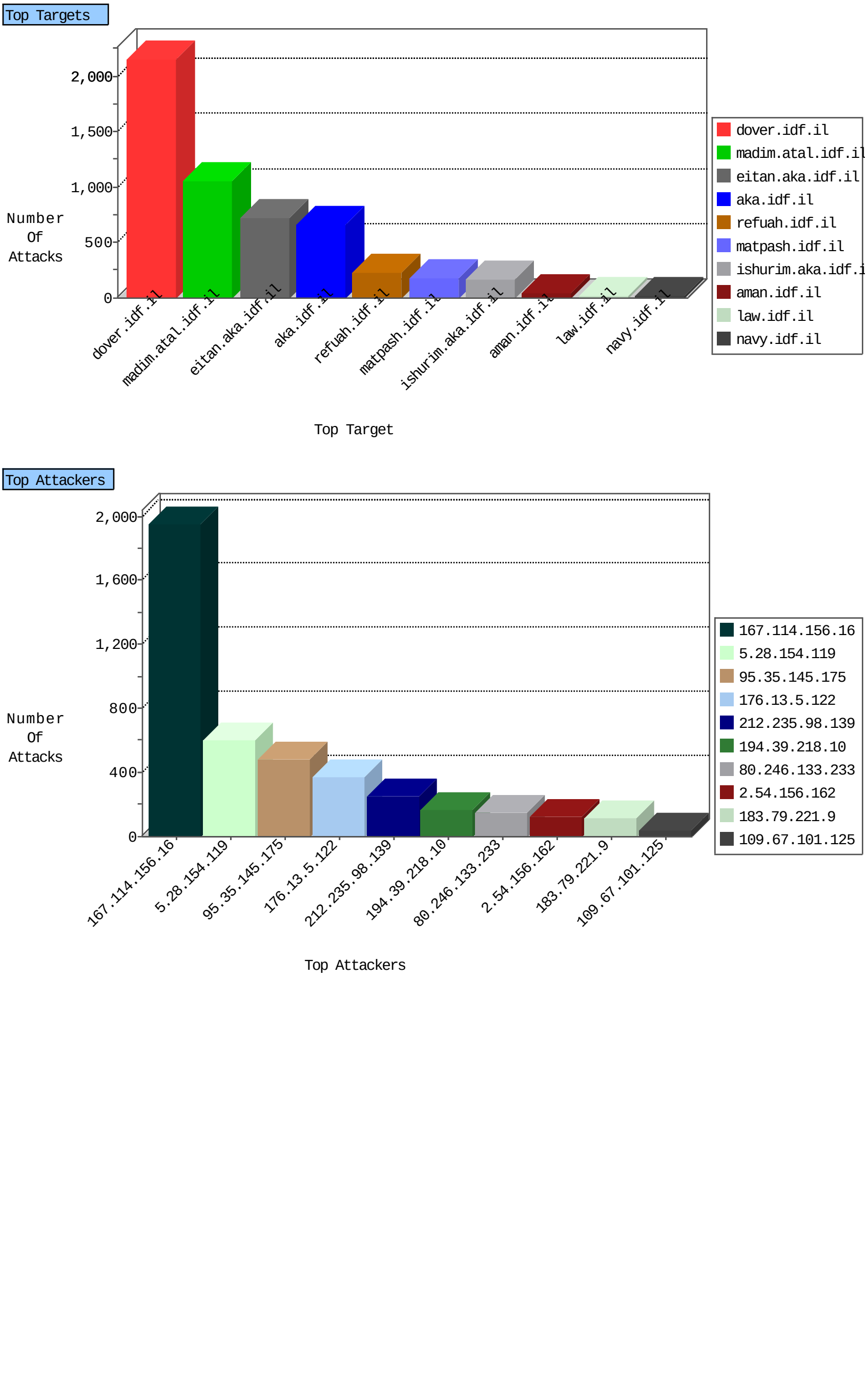
12-14-2015-10:04:00 to 12-14-2015-11:04:00

IDF Under Attack
Daily Report



12-14-2015-10:04:00 to 12-14-2015-11:04:00

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	3610
82.132.212.173	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
181.196.19.30	Ecuador	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
181.196.19.30	Ecuador	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

12-14-2015-10:04:00 to 12-14-2015-11:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.112.102.222		147.237.76.42	refuah.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	7
87.106.179.116	Germany	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
185.112.102.222		147.237.76.42	refuah.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

12-14-2015-10:04:00 to 12-14-2015-11:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.106.179.116	147.237.72.166	Germany	aka.idf.il	SQL Injection - Select From	2
31.168.176.210	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.47.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.165.223	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.112.102.222	147.237.76.42		refuah.idf.il	ET WEB_SERVER Muieblackcat scanner	1
103.38.200.122	147.237.8.45	India	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
84.109.100.38	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.209.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.69	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.0.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.25.102.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
103.38.200.122	147.237.77.243	India	mobile.idf.il	ET SCAN Potential SSH Scan	1
89.138.171.219	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.140.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.63.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.93.60	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

12-14-2015-10:04:00 to 12-14-2015-11:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.28.154.119	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	531
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	252
194.39.218.10	Europe	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	171
80.246.133.233	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	147
183.79.221.9	Japan	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	117
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
84.108.175.188	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
46.19.85.202	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	27
46.19.86.83	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	20
46.19.86.15	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	19
46.19.85.135	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
207.241.229.110	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
213.57.30.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
46.19.85.147	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	15
100.100.16.12		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.205	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
2.52.176.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
109.67.115.55	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
176.12.147.210	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
66.249.65.103	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
213.57.225.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
37.26.149.219	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence		monitor	9
46.19.86.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.114.3.241	Israel	147.237.77.74	law.idf.il	drop	SAM rule	drop	8
176.12.144.77	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
74.63.228.226	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
81.218.154.38	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.205	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.109.76.220	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.248	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
112.198.64.25	Philippines	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.187	Israel	147.237.72.167	ishurim.aka.idf.i	drop	SAM rule	drop	6
62.219.168.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.13.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.248	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.29.213.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.3.144.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.171	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.180.226.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.35.145.175	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid sequence number	alert	5
95.35.145.175	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
185.3.144.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
94.230.86.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.32.179.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
213.57.141.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
77.125.75.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
95.35.145.175	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

12-14-2015-10:04:00 to 12-14-2015-11:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.35.145.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	238
176.13.5.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	188
176.13.5.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	182
95.35.145.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	117
95.35.145.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
2.54.156.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
5.28.154.119	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	72
2.54.156.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
109.67.101.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
37.26.146.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
46.19.86.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
77.126.85.101	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.126.85.101	Block	15
85.64.190.69	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	6
79.178.140.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.111.36.103	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/main/home/default.aspx	Block	3
37.26.147.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
183.79.223.58	Japan	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 183.79.223.58	Block	3
185.3.144.163	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
85.64.190.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	2
109.64.166.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
207.46.13.104	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
84.95.21.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/main/homas	Block	2
80.246.133.233	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
213.151.48.19	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-21486-he/idfgdover.aspx&sa=u&ved=0ahukewj8q_2c-nrjahvnhhokhuracgqqfgghmao&usg=afqjcngoezfbld7n4uxysaj3ci-6ckdomw	Block	1
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method odified-Since: in URL mon,	Block	1
176.12.149.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.187	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-ar/www.idf.il/ar	Block	1
37.142.228.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.141.157	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.156.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.35.94.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-16893-he/dover.aspx	Block	1
176.13.5.221	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Double URL Encoding - parameter: ReturnUrl in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	1
84.109.165.65	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
46.19.85.218	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
147.235.185.74	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/scriptresource.axd	None	1
79.183.116.52	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.204.26	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.26.146.180	Israel	147.237.76.39	mobile.meitav.idf.il	Cookie Tampering on cookie .ASPNETAUTH: Expected 0102105BCF4B6104D308FE10D310176404D3080009320030003900300310039003100300038000012F00FF, Observed 0102C8A5FB9D0DF1D208FEC81D3D6910F1D2080009320030003900300310039003100300038000012F00FF	None	1
95.86.106.28	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/942-5059-he/patzar.aspx&sa=u&ved=0ahukewjuw8rn-drjahwdqxokhdr_bfeqfggimaa&usg=afqjcngfkballpoq07gxlscnwm_l2lawgg	Block	1
62.219.134.126	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
176.13.20.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.51.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.128	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.14	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.150.109	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1

12-14-2015-10:04:00 to 12-14-2015-11:04:00