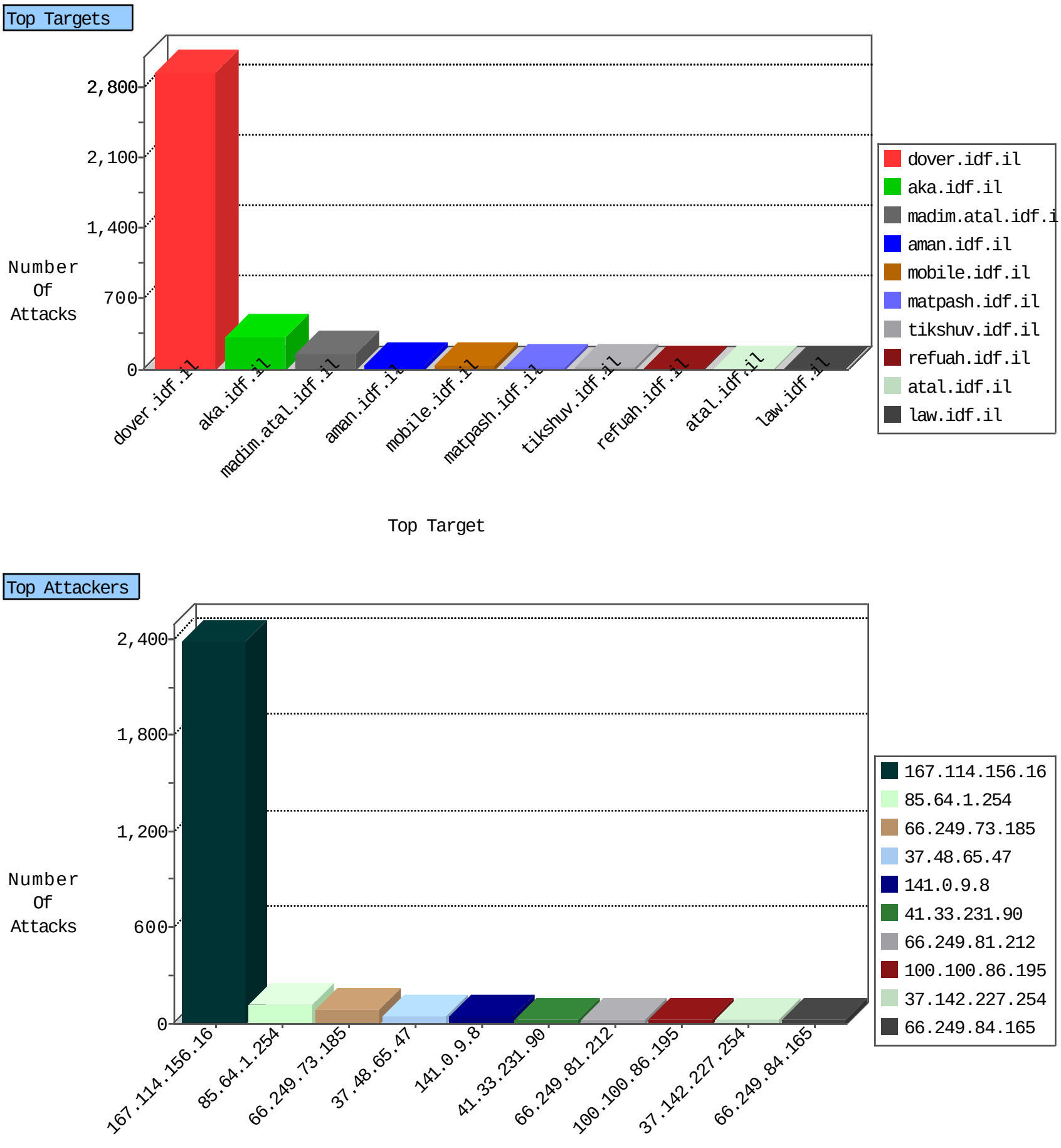
11-27-2015-15:04:05 to 11-27-2015-16:04:05

IDF Under Attack Daily Report



11-27-2015-15:04:05 to 11-27-2015-16:04:05

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	3714
79.180.225.62	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	14
85.65.199.219	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	5
66.240.236.119	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
113.17.175.198	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
82.118.236.47	Bulgaria	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

11-27-2015-15:04:05 to 11-27-2015-16:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.202.102.210	Jordan	147.237.77.216	dover.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	3
111.206.116.217	China	147.237.0.17	m.my-kosher-kravi.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
111.206.116.217	China	147.237.0.19	madim.atal.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
182.50.130.134	Singapore	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-27-2015-15:04:05 to 11-27-2015-16:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	17
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	SERVER-WEBAPP backup access	14
85.65.132.175	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	GPL WEB_SERVER printenv access	2
66.249.66.33	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	GPL EXPLOIT formmail access	2
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	WEB-FRONTPAGE /_vti_bin/ access	2
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	SERVER-WEBAPP printenv access	2
66.249.78.134	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.195	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
112.65.201.60	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
112.64.147.37	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	SERVER-WEBAPP FormHandler.cgi access	1
222.186.21.181	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.181	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	ET WEB_SERVER ColdFusion administrator access	1
180.153.104.125	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	SERVER-WEBAPP server-status access	1
112.65.201.60	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
112.65.201.60	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	SERVER-WEBAPP client negative Content-Length attempt	1
112.64.147.37	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	SERVER-WEBAPP JavaScript tag in User-Agent field possible XSS attempt	1
112.64.147.37	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	POLICY-OTHER Adobe ColdFusion admin interface access attempt	1
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	GPL WEB_SERVER authors.pwd access	1
222.186.21.181	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.76.30	Germany	himush.idf.il	ET SCAN NMAP -sS window 1024	1
31.6.71.154	147.237.77.234	Poland	halag.idf.il	ET SCAN NMAP -sS window 1024	1
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	SERVER-WEBAPP test.cgi access	1
180.153.104.125	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	SERVER-WEBAPP search.cgi access	1
112.65.201.60	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
37.48.65.47	147.237.77.216	Netherlands	dover.idf.il	SERVER-WEBAPP guestbook.cgi access	1

11-27-2015-15:04:05 to 11-27-2015-16:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	86
141.0.9.8	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	43
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
100.100.86.195		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	25
66.249.84.165	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
185.120.126.48		147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	22
37.142.227.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
37.142.227.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
100.100.117.80		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
66.249.73.193	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.75.67.164	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
109.75.67.164	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
37.8.94.216	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
100.100.36.203		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
93.172.116.97	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
41.223.141.80	Botswana	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.39.87.86	France	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
41.223.141.86	Botswana	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.183	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
66.249.83.158	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.228.131.162	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.85.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
96.224.214.237	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.87.240		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
87.68.150.69	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
107.77.70.126	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.2.84		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.83.155	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.223.141.84	Botswana	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.148.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.52	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.69.10.241	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.183	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
66.249.84.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
149.88.3.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
66.249.84.167	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
188.225.185.133	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
213.57.141.14	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
149.88.3.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
2.52.166.216	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.180.21.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

11-27-2015-15:04:05 to 11-27-2015-16:04:05

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
87.68.85.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.54.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.3	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.210.186.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

11-27-2015-15:04:05 to 11-27-2015-16:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.1.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	84
85.64.1.254	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 85.64.1.254	Block	34
37.142.68.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
80.246.137.93	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	11
31.154.0.210	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
80.246.136.53	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/	Block	4
176.13.16.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.182.138.224	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
109.65.75.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	3
185.120.126.106		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
83.223.122.10	United Kingdom	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &y in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	2
46.19.85.51	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
40.77.167.91	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.64.218.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.228.64.43	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
93.172.116.97	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.160.253.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.63.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.250.138.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.39.87.86	France	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
54.159.37.195	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
85.250.207.207	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
77.127.214.146	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
5.102.246.130	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 5.102.246.130	Block	1
84.228.196.187	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
109.66.136.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.166.53	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
197.35.187.191	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.64.3	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.64.3	Block	1
94.159.155.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.68.150.69	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.179.114.184	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
176.13.8.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
111.206.116.217	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/loginaction!login.action	Block	1
85.65.157.249	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.151	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-9301-he/dover.aspx	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized Method GET for www.aka.idf.il/rights/asp/searchresults.asp	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
5.29.122.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.19.253	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ufi/reaction/	Block	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
2.54.24.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.14.182	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	1
176.106.226.210	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
46.121.30.33	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.172.41.107	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
77.237.138.51	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1

11-27-2015-15:04:05 to 11-27-2015-16:04:05