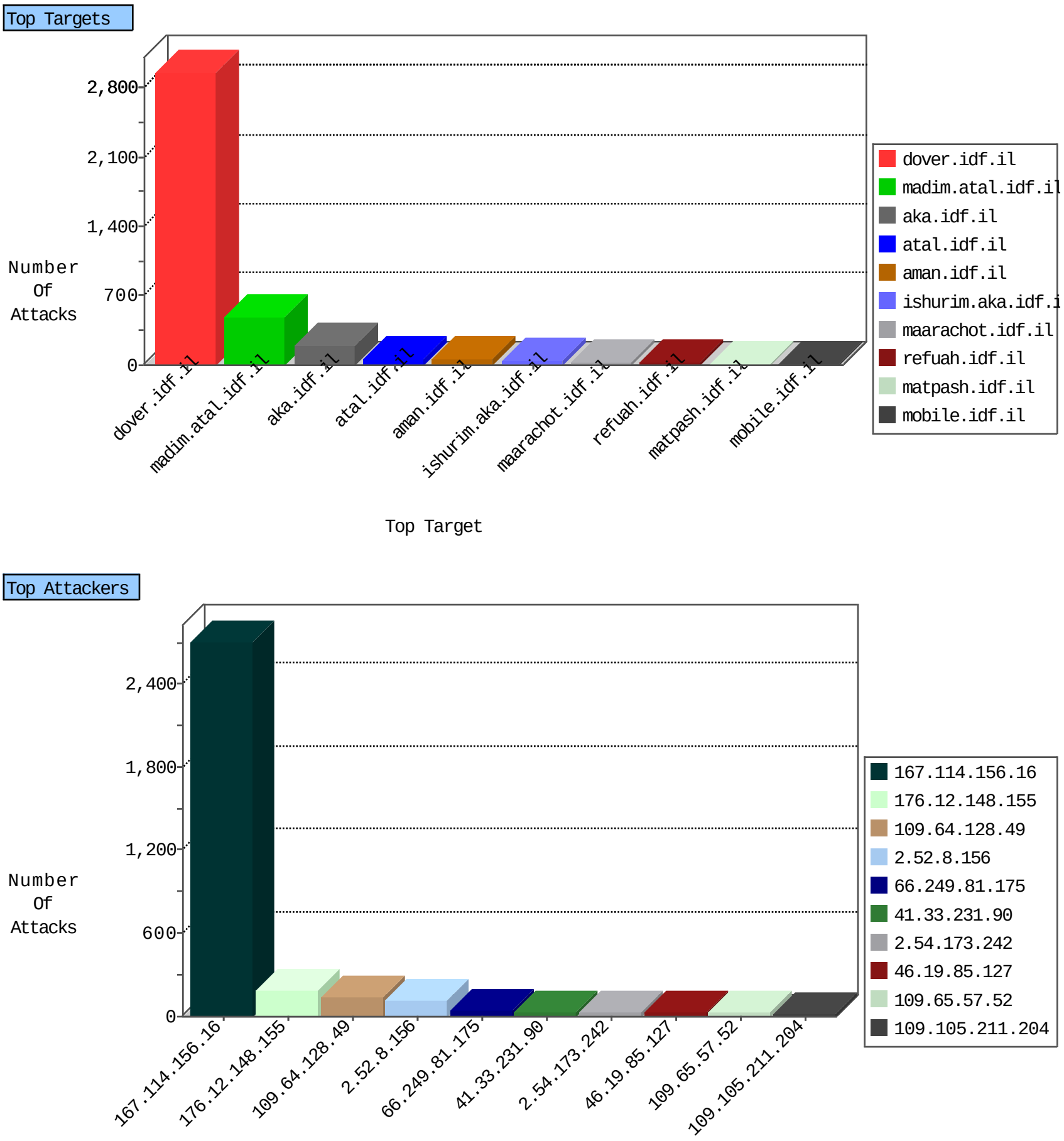
12-04-2015-09:04:08 to 12-04-2015-10:04:08

IDF Under Attack
Daily Report



12-04-2015-09:04:08 to 12-04-2015-10:04:08

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	3327
77.75.74.41	Czech Republic	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
204.42.253.2	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	2
118.193.21.98	China	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
202.112.51.96	China	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
202.112.51.96	China	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
180.97.106.36	China	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
118.193.21.98	China	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
202.112.51.96	China	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1

12-04-2015-09:04:08 to 12-04-2015-10:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-04-2015-09:04:08 to 12-04-2015-10:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.18	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	16
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
176.12.148.155	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
109.105.211.204	147.237.76.202	Bosnia and Herzegovina	e.halag.idf.il	ET SCAN Potential SSH Scan	2
66.249.81.175	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
109.105.211.204	147.237.77.176	Bosnia and Herzegovina	matpash.idf.il	ET SCAN Potential SSH Scan	2
209.126.116.147	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
109.105.211.204	147.237.76.30	Bosnia and Herzegovina	himush.idf.il	ET SCAN Potential SSH Scan	1
109.105.211.204	147.237.72.166	Bosnia and Herzegovina	aka.idf.il	ET SCAN Potential SSH Scan	1
109.105.211.204	147.237.77.226	Bosnia and Herzegovina	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
109.105.211.204	147.237.0.15	Bosnia and Herzegovina	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.105.211.204	147.237.77.61	Bosnia and Herzegovina	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.72.156	Canada	aman.idf.il	ET SCAN NMAP -f -sS	1
98.226.32.142	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
109.105.211.204	147.237.76.197	Bosnia and Herzegovina	e.himush.idf.il	ET SCAN Potential SSH Scan	1
98.226.32.142	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
109.105.211.204	147.237.76.176	Bosnia and Herzegovina	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
98.226.32.142	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
109.105.211.204	147.237.76.44	Bosnia and Herzegovina	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
109.105.211.204	147.237.76.31	Bosnia and Herzegovina	nakchal.idf.il	ET SCAN Potential SSH Scan	1
109.105.211.204	147.237.72.217	Bosnia and Herzegovina	e.idf.il	ET SCAN Potential SSH Scan	1
109.105.211.204	147.237.77.233	Bosnia and Herzegovina	atal.idf.il	ET SCAN Potential SSH Scan	1
109.105.211.204	147.237.0.19	Bosnia and Herzegovina	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.72.156	Canada	aman.idf.il	ET SCAN NMAP -sS window 2048	1
109.105.211.204	147.237.77.19	Bosnia and Herzegovina	law-forum.idf.il	ET SCAN Potential SSH Scan	1
98.226.32.142	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
109.105.211.204	147.237.76.199	Bosnia and Herzegovina	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
98.226.32.142	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
109.105.211.204	147.237.76.177	Bosnia and Herzegovina	ncore.idf.il	ET SCAN Potential SSH Scan	1
98.226.32.142	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
109.105.211.204	147.237.76.86	Bosnia and Herzegovina	navy.idf.il	ET SCAN Potential SSH Scan	1
98.226.32.142	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
109.105.211.204	147.237.76.39	Bosnia and Herzegovina	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1

12-04-2015-09:04:08 to 12-04-2015-10:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.81.175	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	41
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
109.65.57.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.85.127	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	20
46.19.86.93	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	17
100.100.48.52		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.2	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
77.125.147.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.173.242	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
2.54.173.242	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	10
113.87.123.167	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
84.228.210.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.173	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.132.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
100.100.15.0		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.200.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.228.200.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.156	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.68	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.156	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.10	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.81.179	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
109.226.26.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.173.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.145.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.173.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.173.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
109.64.128.49	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.169.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.164.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
91.221.59.25	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
84.228.249.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.21.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.226.26.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.179.114.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.145.92	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.221.59.25	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.54.179.142	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.180.168.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.128.197	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.183.197.137	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3

12-04-2015-09:04:08 to 12-04-2015-10:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.8.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	109
176.12.148.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
109.64.128.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	72
176.12.148.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	72
109.64.128.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	41
109.64.128.49	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.64.128.49	Block	26
2.54.155.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
176.12.148.155	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.12.148.155	Block	14
2.52.8.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	12
85.65.55.39	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 85.65.55.39	Block	6
2.54.185.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
50.87.2.93	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
79.182.227.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.109.75.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	3
109.186.32.195	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2
39.41.195.219	Pakistan	147.237.77.74	law.idf.il	PHP Attempt	Block	2
93.173.226.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.32.179.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
39.41.195.219	Pakistan	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	2
95.86.65.9	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	2
50.87.2.93	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
2.52.16.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
82.166.242.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	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
50.87.2.93	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	2
93.172.141.56	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method Â²$Ã¦[[#22]]j[[#4]]Ã…[[#31]]Ã-Ã¹DÃ“[[#31]]gÃ“[[#25]] in URL	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20451-he/dover.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
87.68.244.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.98	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
84.228.200.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.81.138	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
37.26.146.221	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
185.3.144.101	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
93.172.141.56	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method Â²$Ã¦[[#22]]j[[#4]]Ã…[[#31]]Ã-Ã¹DÃ“[[#31]]gÃ“[[#25]]	Block	1
85.65.55.39	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/2/size338x0/1802.jpg	Block	1
50.87.52.131	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 50.87.52.131	Block	1
173.252.74.121	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.128.49	Israel	147.237.0.19	madim.atal.idf.i	Too Many 404: Response Code per Session	Block	1
2.54.167.122	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.67.196	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/usercontrols/headerupper/	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/69037.pdf	Block	1
176.13.10.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.172.19.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
50.87.2.93	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 50.87.2.93	Block	1
113.87.123.167	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1

12-04-2015-09:04:08 to 12-04-2015-10:04:08