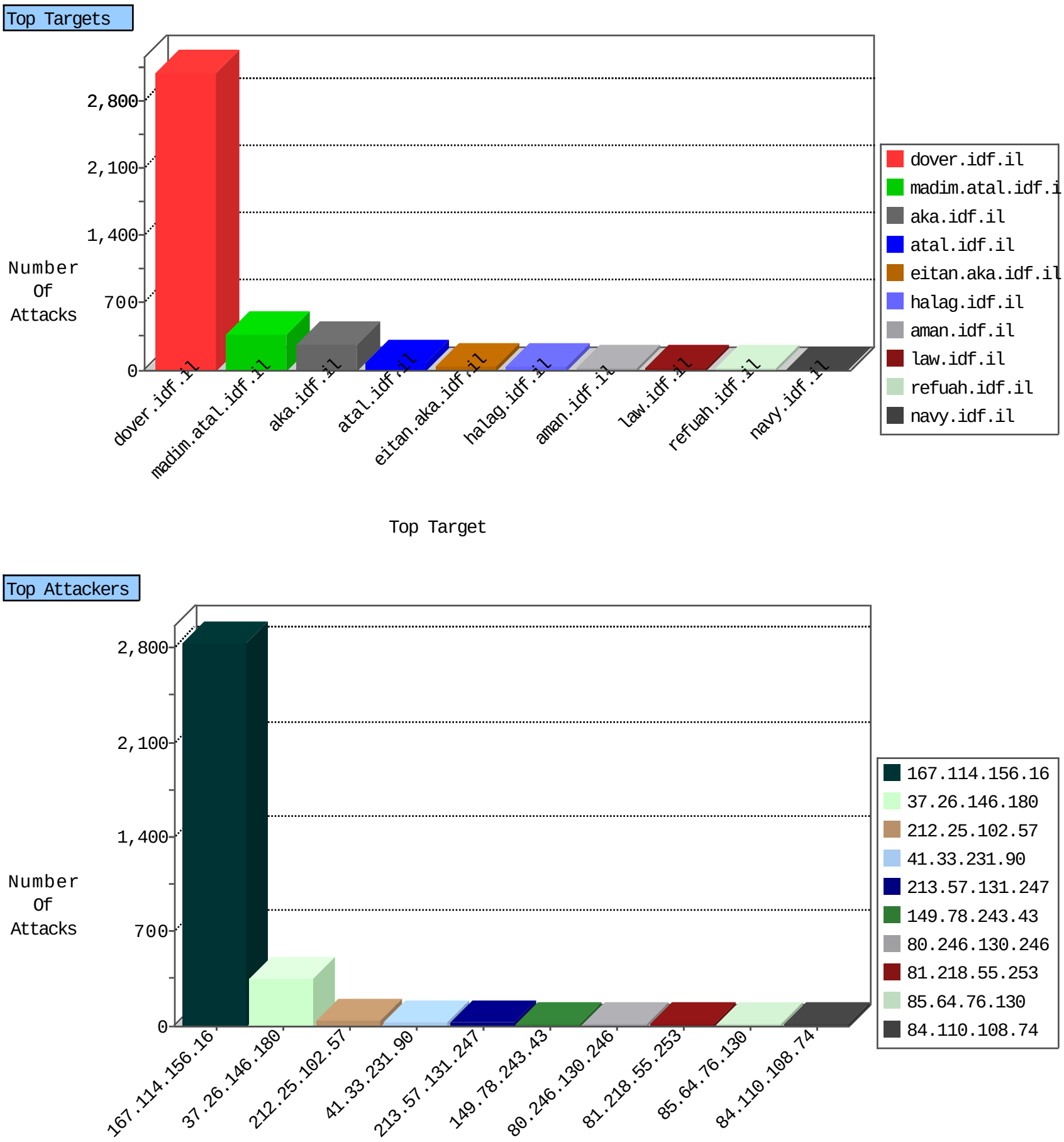
12-03-2015-18:04:00 to 12-03-2015-19:04:00

IDF Under Attack Daily Report



12-03-2015-18:04:00 to 12-03-2015-19:04:00

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	3580
94.102.56.238	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
94.102.56.238	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
94.102.56.238	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
94.102.56.238	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
94.102.56.238	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
94.102.56.238	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
192.3.170.124	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
94.102.56.238	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

12-03-2015-18:04:00 to 12-03-2015-19:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.142	Italy	147.237.76.147	chinuch.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1
151.80.31.150	Italy	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1

12-03-2015-18:04:00 to 12-03-2015-19:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.106.94.46	147.237.76.42		refuah.idf.il	ET SCAN NMAP -sS window 1024	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.171.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.52.225	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.34.154	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
204.13.204.139	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 2048	1
200.35.150.97	147.237.76.38	Panama	e.e.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
185.106.94.46	147.237.76.44		e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.14.79	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.50.146.135	147.237.72.217	Italy	e.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.93.191	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
204.13.204.139	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 3072	1
204.13.204.139	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -f -sS	1

12-03-2015-18:04:00 to 12-03-2015-19:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
149.78.243.43	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
80.246.130.246	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
89.139.55.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.57.131.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
100.100.116.203		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
81.218.55.253	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
213.57.131.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
66.249.66.45	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.86.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.121.40.123	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
81.218.55.253	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
31.168.226.186	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.133.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.133.112.193	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.110.108.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.160.245.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.57.61.92	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.254	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.134.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.160.245.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
100.100.0.64		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.187	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
100.100.0.64		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
62.219.193.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.204.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.61.92	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.182.129.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.64.76.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.64.3.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
85.64.76.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
46.19.86.147	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.64.3.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.183.146.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.64.3.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
5.102.254.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.39.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.64.76.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
69.171.228.123	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
176.12.150.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
69.171.228.116	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
213.57.131.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
31.13.102.123	Ireland	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4

12-03-2015-18:04:00 to 12-03-2015-19:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.180	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.146.180	Block	139
37.26.146.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
37.26.146.180	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 37.26.146.180	Block	90
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	40
188.165.234.52	France	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 188.165.234.52	Block	11
176.228.40.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.19.86.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
81.24.209.144	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	3
84.228.0.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.98.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.0.73	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
79.180.180.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
37.142.64.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.3.128	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
184.161.241.203	Canada	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	2
157.55.39.243	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
41.69.251.43	Egypt	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
157.55.39.18	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12847-he/dover.aspx×³Â¡×³Â?"×³Ö³Æ'Ö¶â€™Ö³â€ ×'â,¬â„¢Ö³Æ'×'â,¬Â Ö³Â¢×'â€šÂ¬×'â€žÂ¢Ö³Æ'Ö¶â€™Ö³Â¢×'â€šÂ¬ÖµÂ¡Ö³Æ'×'â,¬ÂšÖ³â€šÖ²Â¯Ö³Æ'Ö¶â€™Ö³â€ ×'â,¬â„¢Ö³Æ'Ö²Â¢Ö³Â¢×'â,¬ÂšÖ²Â¬Ö³â€¦Ö²Â¡Ö³Æ'Ö¶â€™Ö³Â¢×'â€šÂ¬ÖµÂ¡Ö³Æ'×'â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ'Ö¶â€™Ö³â€ ×'â,¬â„¢Ö³Æ'Ö²Â¢Ö³Â¢×'â,¬ÂšÖ²Â¬Ö³â€¦Ö²Â¡Ö³Æ'Ö¶â€™Ö³Â¢×'â€šÂ¬ÖµÂ¡Ö³Æ'×'â,¬ÂšÖ³â€šÖ²Â½	Block	1
79.176.103.113	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.176.103.113	Block	1
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	1
37.26.148.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.152.216	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.31	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ the idf official website	Block	1
185.32.179.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.35.54.170	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
46.19.85.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.243	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter v in www.eitan.aka.idf.il/styles/styles_orange.css	None	1
109.160.245.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.68.73	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
37.26.146.180	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
95.133.210.184	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1
198.20.69.74	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
176.13.19.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.119.4	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
46.19.85.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.115	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
81.218.55.253	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
79.176.103.113	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
207.46.13.51	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/default.aspx	Block	1
37.142.64.63	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed PHP Attempt	Block	1
109.65.141.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/main/rabanut/general.aspx	None	1
188.53.61.172	Saudi Arabia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
95.35.54.170	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 95.35.54.170	None	1
46.19.86.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.12.142.88	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1
41.66.46.216	Cote D'Ivoire	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1

12-03-2015-18:04:00 to 12-03-2015-19:04:00