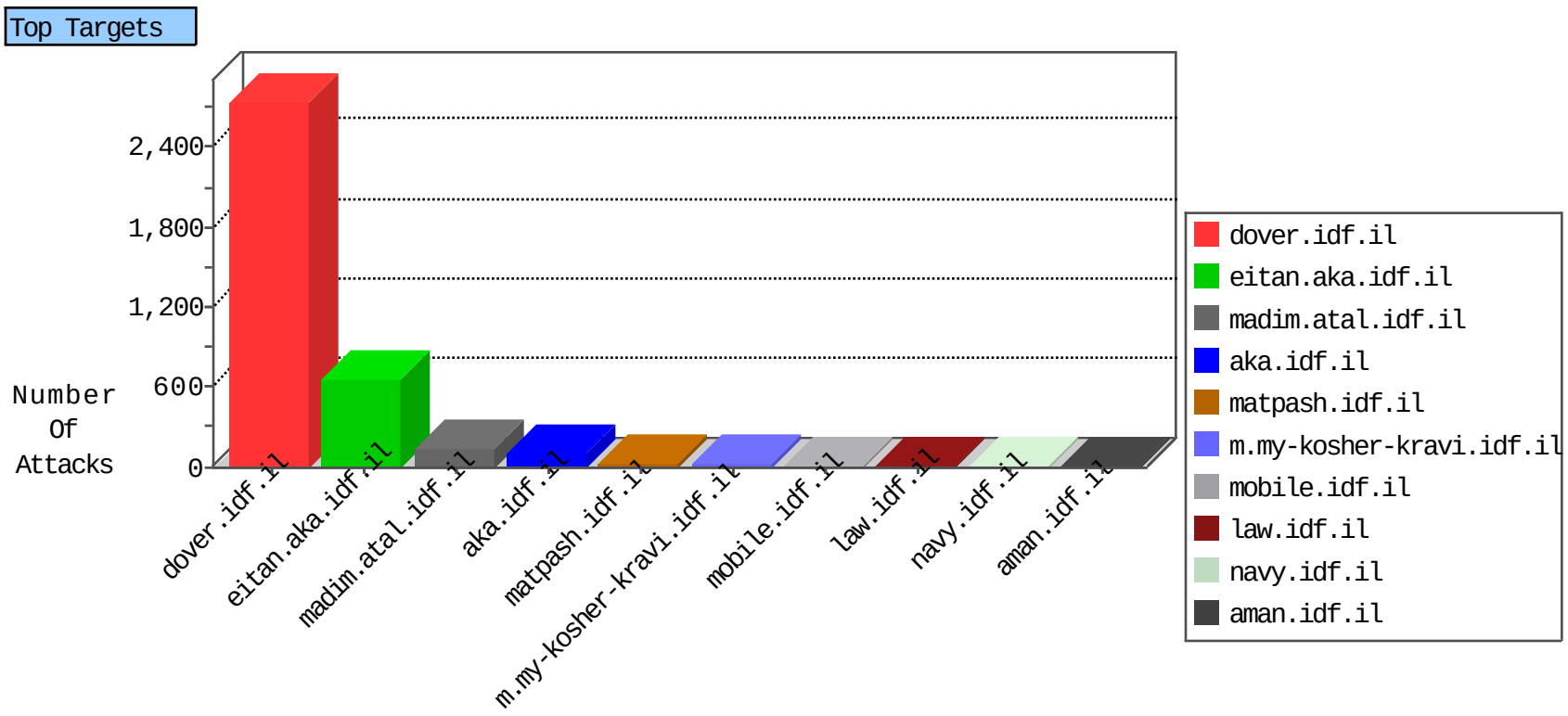
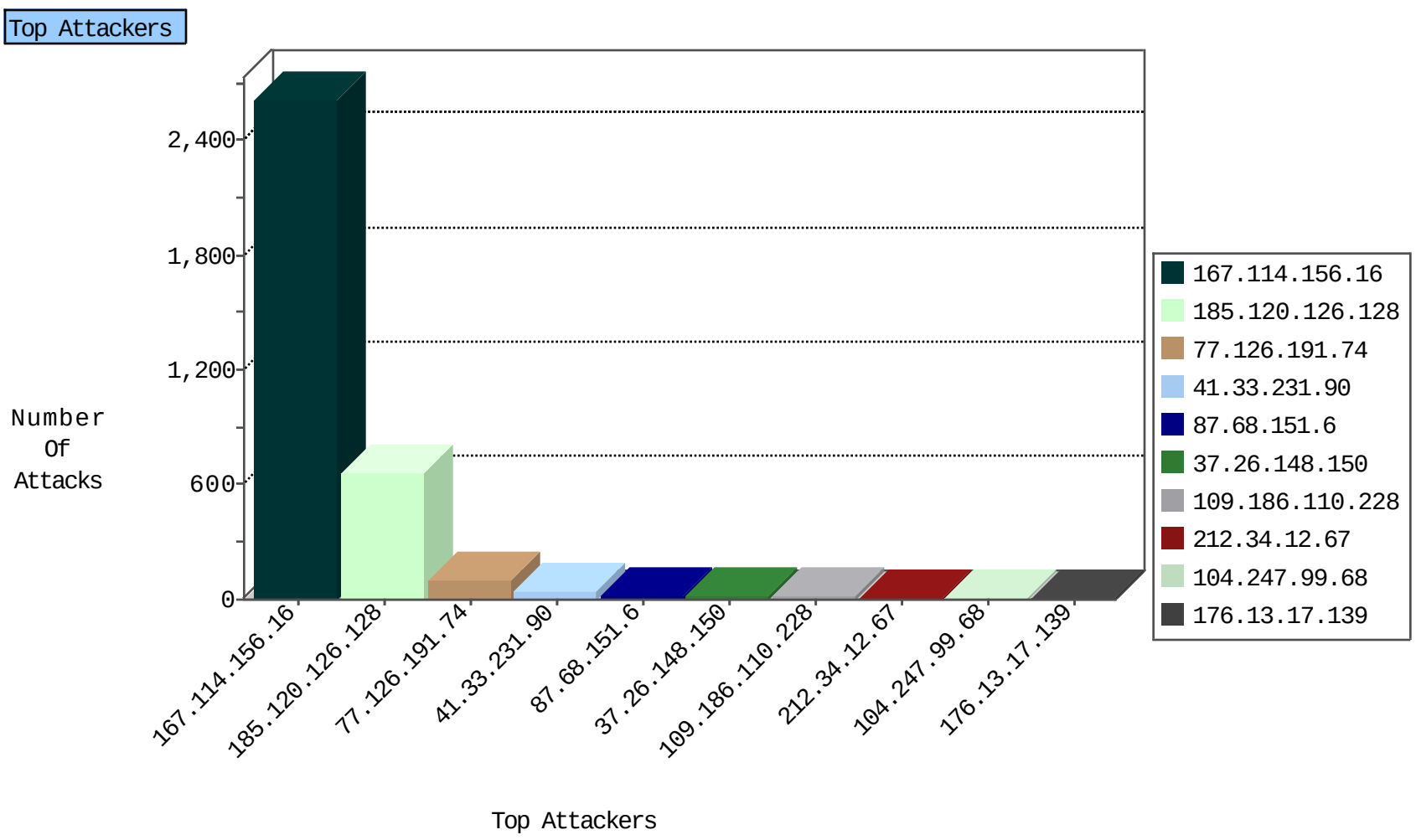
12-12-2015-09:04:04 to 12-12-2015-10:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



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

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	3476
204.42.253.132	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
88.206.95.80	Russian Federation	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
178.137.145.176	Ukraine	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

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

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
197.220.162.4	147.237.72.166	Ghana	aka.idf.il	ET SCAN Potential SSH Scan	1
23.95.113.154	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
197.220.162.4	147.237.72.14	Ghana	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
23.95.113.154	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
193.104.41.54	147.237.77.121	Moldova, Republic of	e.navy.idf.il	ET SCAN Potential SSH Scan	1
23.95.113.154	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
193.104.41.54	147.237.76.198	Moldova, Republic of	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
193.104.41.54	147.237.72.167	Moldova, Republic of	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
193.104.41.54	147.237.0.19	Moldova, Republic of	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
119.146.221.68	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
220.178.78.138	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
61.238.90.246	147.237.8.28	Hong Kong	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
197.220.162.4	147.237.72.167	Ghana	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
23.95.113.154	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
197.220.162.4	147.237.72.156	Ghana	aman.idf.il	ET SCAN Potential SSH Scan	1
23.95.113.154	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
23.95.113.154	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
193.104.41.54	147.237.76.200	Moldova, Republic of	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
193.104.41.54	147.237.76.42	Moldova, Republic of	refuah.idf.il	ET SCAN Potential SSH Scan	1
193.104.41.54	147.237.8.27	Moldova, Republic of	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
159.122.238.133	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
220.178.78.138	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
119.146.221.68	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
197.220.162.4	147.237.72.217	Ghana	e.idf.il	ET SCAN Potential SSH Scan	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.126.128		147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	570
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.26.148.150	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	20
109.186.110.228	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
104.247.99.68		147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	7
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.162.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.186.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.108.244.70	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
185.32.179.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
149.88.230.98	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
207.241.226.39	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
62.0.110.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.182.49.164	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.17.139	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.112.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.106.46.67	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
149.78.240.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.177.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.59.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
207.46.13.57	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.137.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
84.228.84.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.164.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.120.46.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.135.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
169.229.3.90	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
162.247.72.201	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
188.120.148.152	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.108.16.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.163	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.3.146.200	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
183.79.219.108	Japan	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
128.232.110.28	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.120.194.205	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
188.120.148.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.106.46.67	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.120.202.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
5.102.254.225	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.120.46.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
157.55.39.173	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
77.126.191.74	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	2
176.13.21.201	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Bad TCP sequence	Invalid ACK number	alert	2

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

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.120.202.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.116.130.156	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.120.126.128		147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 185.120.126.128	Block	84
77.126.191.74	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	56
77.126.191.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
87.68.151.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
77.126.191.74	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 77.126.191.74	Block	17
176.13.17.139	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
46.19.85.163	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
77.125.146.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.68.151.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
212.34.12.67	Jordan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 212.34.12.67	Block	2
79.177.180.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.250.92.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.34.12.67	Jordan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 212.34.12.67	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
77.126.191.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
176.12.141.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	2
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
84.94.37.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
207.46.13.57	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/	Block	1
66.249.66.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
176.12.144.16	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 176.12.144.16	Block	1
37.142.186.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
146.185.234.48	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	1
84.108.220.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.34.12.67	Jordan	147.237.77.176	matpash.idf.il	Multiple Malformed URL from 212.34.12.67	Block	1
188.2.4.160		147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
176.12.139.110	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
66.249.66.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
2.52.63.147	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
207.46.13.171	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/1/size220x0/17451.jpg	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1405-he/atal.aspx	Block	1
146.185.234.48	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
212.34.12.67	Jordan	147.237.77.176	matpash.idf.il	Multiple Unknown HTTP Request Method from 212.34.12.67	Block	1
188.143.232.13	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-19112-en/dover.aspx	Block	1
176.12.139.110	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.12.139.110	None	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/kamiljenin.aspx	Block	1
5.79.68.161	Netherlands	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	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
79.181.164.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/default	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
185.120.126.128		147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1
157.55.39.173	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.121.253	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
212.34.12.67	Jordan	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method e/webp,*/*;q=0.8 in URL	Block	1
66.249.66.132	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list2005b.htm	Block	1
36.229.176.163	Taiwan	147.237.77.216	dover.idf.il	Directory Traversal (In URL)	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

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