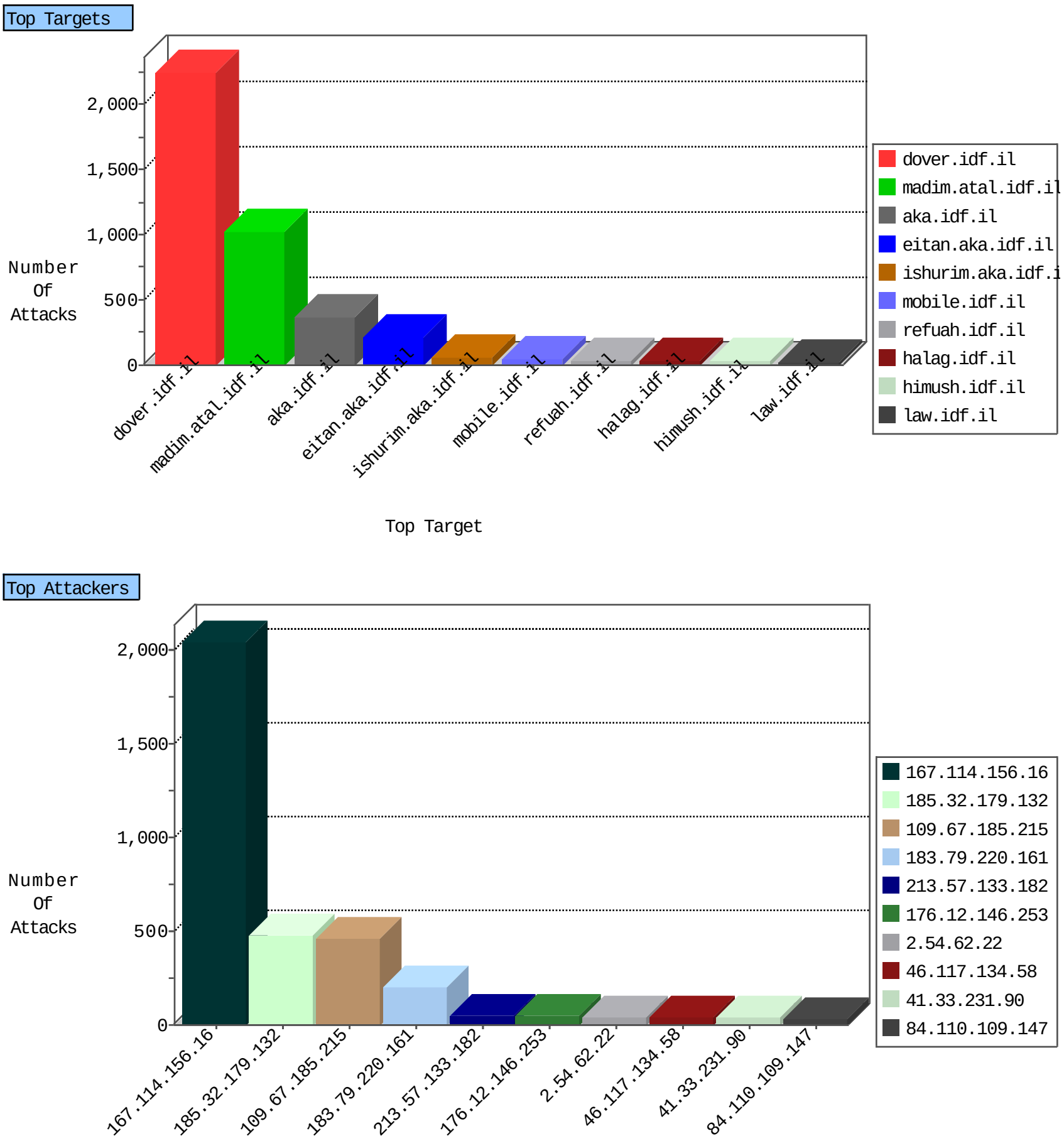
12-14-2015-19:04:04 to 12-14-2015-20:04:04

IDF Under Attack
Daily Report



12-14-2015-19:04:04 to 12-14-2015-20:04:04

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	3222
77.126.12.58	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
79.178.54.173	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
52.53.222.9	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1

12-14-2015-19:04:04 to 12-14-2015-20:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-14-2015-19:04:04 to 12-14-2015-20:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.32.179.132	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.246.133.192	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
124.195.216.105	147.237.72.166	Maldives	aka.idf.il	portscan: TCP Distributed Portscan	1
23.97.172.218	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
112.196.49.101	147.237.76.44	India	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
5.29.53.246	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
89.139.6.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
221.231.6.246	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.77.227	United States	e.hamaz.idf.il	ET DROP Dshield Block Listed Source	1
60.169.78.38	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.7	147.237.0.15	Ukraine	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
60.169.78.38	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
23.97.172.218	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential SSH Scan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
23.97.172.218	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.76.44	India	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
23.97.172.218	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
109.200.157.163	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
5.28.150.20	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.172.164.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.250.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.234.18.210	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.178.114.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
60.169.78.38	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
192.228.132.151	147.237.76.30	Malaysia	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
23.97.172.218	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
177.245.32.84	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
23.97.172.218	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1

12-14-2015-19:04:04 to 12-14-2015-20:04:04

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
183.79.220.161	Japan	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
84.110.109.147	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
2.54.62.22	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
213.57.133.182	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	15
77.126.12.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
213.57.133.182	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
213.57.133.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
79.176.206.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.180.168.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.184.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.22.131.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.46.39.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.102.254.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
77.127.233.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.133.182	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.160.167.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.90.210.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.57.133.182	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.116.186.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.116.186.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
213.57.133.182	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
109.67.177.125	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.116.186.196	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
188.120.148.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.116.186.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.62.22	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
31.210.186.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.117.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.62.22	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.142.64.73	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.7	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
213.57.137.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.116.186.196	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.62.22	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
77.126.12.58	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.102.254.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.66.123.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
5.29.236.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.98	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
80.246.136.37	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

12-14-2015-19:04:04 to 12-14-2015-20:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	301
109.67.185.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	244
185.32.179.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
109.67.185.215	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 109.67.185.215	Block	115
109.67.185.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
183.79.220.161	Japan	147.237.76.200	eitan.aka.idf.il	Multiple Abnormally Long Request from 183.79.220.161	Block	83
183.79.220.161	Japan	147.237.76.200	eitan.aka.idf.il	Multiple Illegal HTTP Version from 183.79.220.161	Block	83
176.12.146.253	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	49
185.32.179.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	44
46.117.134.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
95.35.173.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
37.26.146.190	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
91.200.12.106	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	12
91.200.12.106	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 91.200.12.106	Block	11
2.52.176.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
109.64.160.140	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	7
2.54.4.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
104.197.184.168	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 104.197.184.168	Block	6
91.200.12.18	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
91.200.12.18	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.200.12.18	Block	5
185.32.179.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
213.57.225.166	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	4
2.52.54.81	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
5.29.53.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	3
84.109.68.86	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
79.179.197.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.12.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.78.216.107	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
109.66.28.158	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
46.60.56.206	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
2.54.0.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
94.230.86.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	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
173.252.88.92	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	2
149.78.179.136	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	2
95.86.71.245	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.66.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
84.110.109.147	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
213.8.204.49	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
54.153.33.152	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
46.19.85.18	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.180.25.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.34	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/ajax/visit_log	Block	1
2.54.184.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.73.165	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.77	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9688-he/refuah.aspx	Block	1
173.252.90.124	United States	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	1

12-14-2015-19:04:04 to 12-14-2015-20:04:04