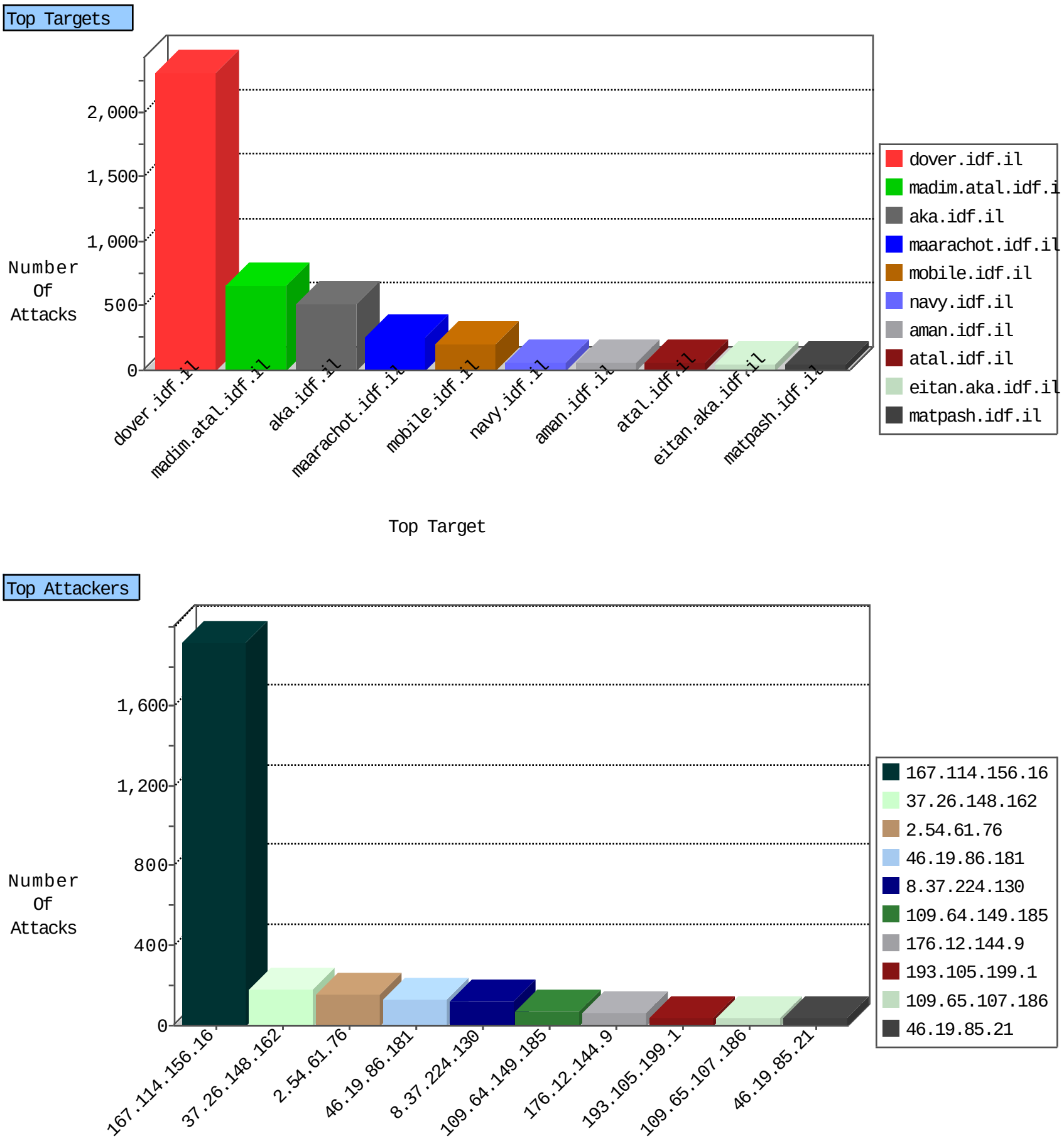
01-04-2016-13:04:08 to 01-04-2016-14:04:08

IDF Under Attack Daily Report



01-04-2016-13:04:08 to 01-04-2016-14:04:08

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	3183
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	478
141.0.14.73	Europe	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	3
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	3
8.37.224.130	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
141.0.14.73	Europe	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
106.75.199.186	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

01-04-2016-13:04:08 to 01-04-2016-14:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.243	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

01-04-2016-13:04:08 to 01-04-2016-14:04:08

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	2
180.150.177.188	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.238	147.237.0.19		madim.atal.idf.il	ET SCAN NMAP -f -sS	1
89.228.27.16	147.237.72.166	Poland	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.112.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.101.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.37.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.224	147.237.76.199		e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
172.98.200.238	147.237.0.19		madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
103.31.80.226	147.237.76.176	Pakistan	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
84.228.184.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.98.162	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.121.167	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.208	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1

01-04-2016-13:04:08 to 01-04-2016-14:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.61.76	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	159
109.64.149.185	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	70
8.37.224.130	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
8.37.224.130	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	56
193.105.199.1	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
109.65.107.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
213.175.183.170	Lebanon	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
132.74.211.4	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
204.118.135.32	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	21
185.79.100.61		147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	19
82.81.37.75	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.54.144.211	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
89.138.110.141	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
62.180.231.212	Europe	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	16
79.177.223.224	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.160.166.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
72.37.140.43	Italy	147.237.72.166	aka.idf.il	drop	SAM rule	drop	14
109.160.166.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
31.168.23.179	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	13
80.179.13.39	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
212.143.36.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.114.23.209	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
85.130.130.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.160.179.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
192.118.11.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
217.194.195.181	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
37.26.147.211	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
62.0.200.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
141.0.14.73	Europe	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	10
81.218.241.26	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
109.64.189.134	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
2.54.179.149	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
132.74.216.147	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
31.168.227.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
62.0.200.108	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	7
2.54.52.33	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
5.102.254.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
132.64.214.207	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
37.26.148.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.160	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.162.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.81.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.24	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.117.244.214	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
80.178.189.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

01-04-2016-13:04:08 to 01-04-2016-14:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	98
37.26.148.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	93
37.26.148.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
176.12.144.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
46.19.85.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
46.19.85.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
46.19.85.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
185.32.179.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
109.253.200.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
46.19.86.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	28
46.19.85.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
37.26.146.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
185.32.179.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
80.246.139.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
80.178.169.13	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 80.178.169.13	Block	12
46.19.85.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
46.19.85.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.52.154.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
209.88.173.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	3
80.246.139.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.126.69.60	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.126.69.60	Block	3
185.32.179.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.7.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.204.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.160	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	3
192.118.11.120	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.118.11.120	Block	3
109.253.136.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
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	2
176.13.17.147	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
46.19.86.52	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
37.142.147.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
81.218.154.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/tfasim.asbx	Block	2
192.114.2.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
79.182.164.187	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.111.248.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
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	2
185.32.179.110	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
109.65.34.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.118.11.120	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/selectusertype.asp	Block	2
46.19.85.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.179.202.129	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.65.107.186	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
5.29.101.17	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash/login/+	Block	1
80.246.136.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.31	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	1
176.13.3.108	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1133-he/atal.aspx	Block	1
2.52.156.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.178.136.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1

01-04-2016-13:04:08 to 01-04-2016-14:04:08