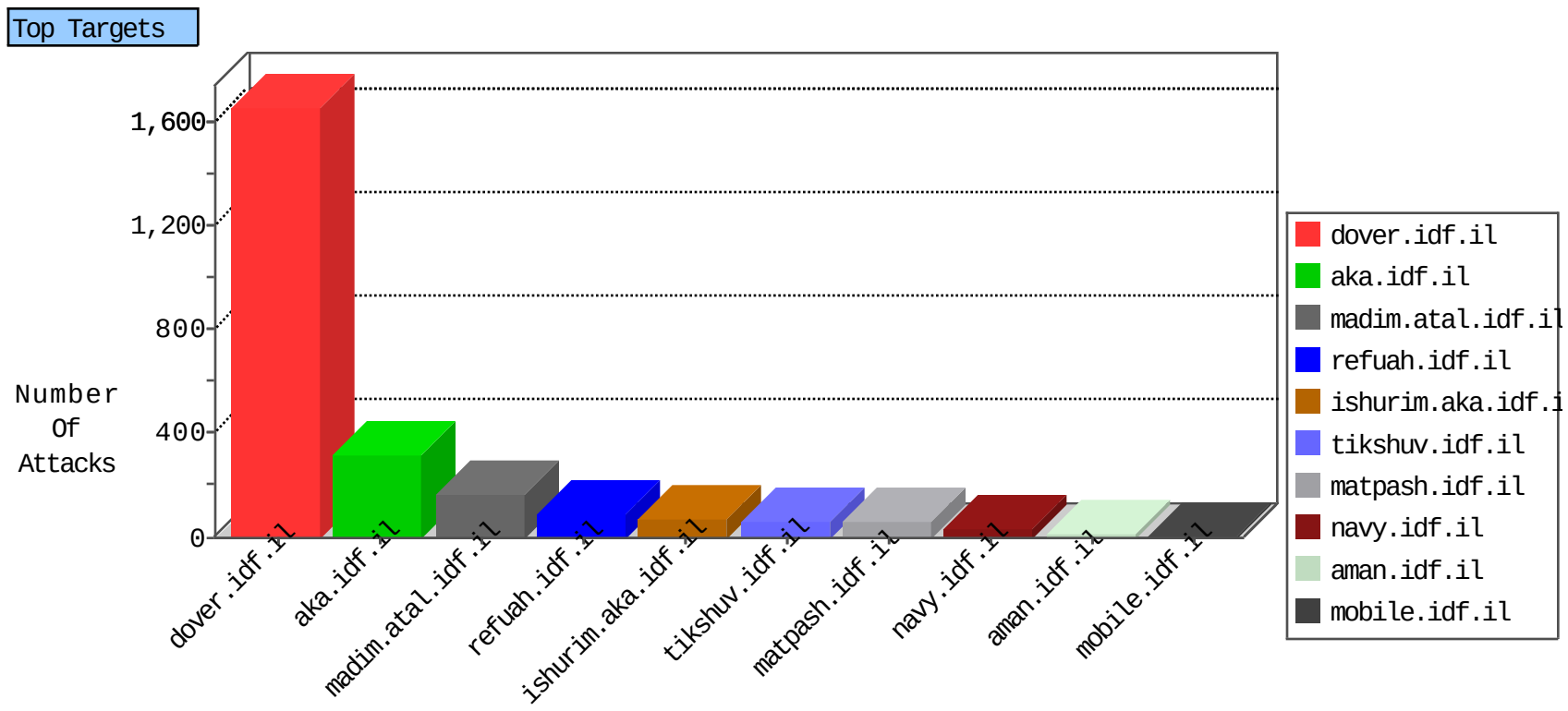
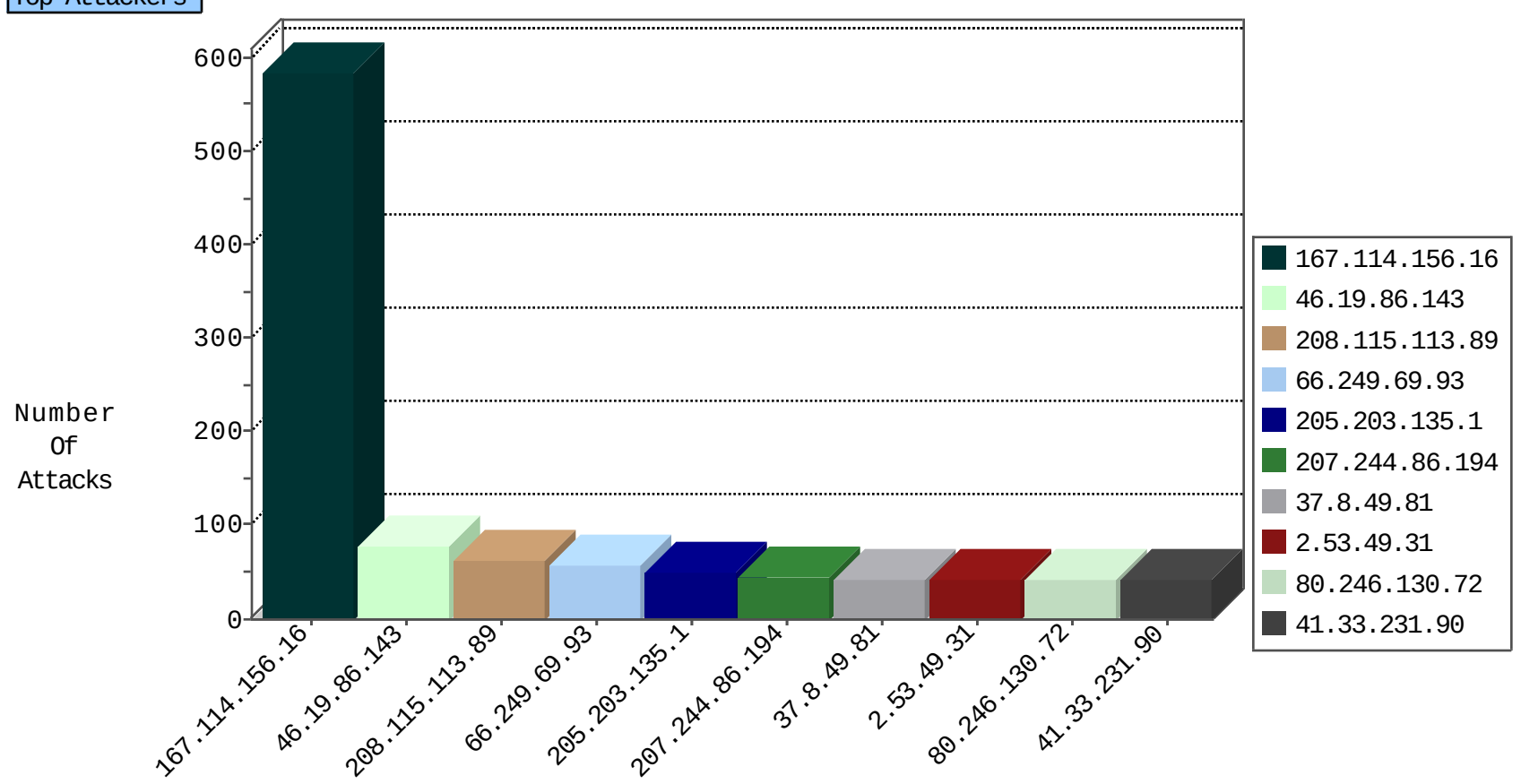
04-21-2016-11:04:03 to 04-21-2016-12:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-21-2016-11:04:03 to 04-21-2016-12:04:03

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	TCP handshake violation, first packet not syn	drop	1133
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1077
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	572
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	107
185.32.179.10	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	26
79.182.41.196	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
149.78.48.81	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
212.199.61.93	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
146.185.57.8	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
89.46.102.242	Romania	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
109.226.51.150	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
199.203.215.1	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

04-21-2016-11:04:03 to 04-21-2016-12:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.8.49.81	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	12132: HTTP: BOIC DoS Tool	Block	43
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	1

04-21-2016-11:04:03 to 04-21-2016-12:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.119	147.237.77.216	Europe	dover.idf.il	ET SCAN NMAP -sA (2)	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
219.83.163.168	147.237.76.38	China	e.e.meitav.idf.i	ET SCAN Potential SSH Scan	1
212.235.66.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.154.54.169	147.237.76.199	France	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
149.88.88.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.139.167	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.228.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.89.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.18.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
221.182.29.55	147.237.0.19	China	madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
213.8.204.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.228.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.27.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-21-2016-11:04:03 to 04-21-2016-12:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	261
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
207.244.86.194	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
83.236.157.245	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
80.246.130.72	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	41
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	31
83.185.244.1	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
213.244.81.60	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
74.6.254.127	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
109.65.110.173	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
2.55.165.232	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
37.142.201.160	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
212.29.225.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
195.160.242.40	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
213.8.204.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
195.160.242.40	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
46.18.17.136	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
79.181.103.160	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
185.6.56.174	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.177.229.6	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.55.169.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
50.116.30.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.102.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.55.0.0	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.53.57.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
213.8.204.56	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
185.89.217.228	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
207.46.13.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.167.25	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.211.52.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.0.99.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
40.77.167.80	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.200.45.155	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.176.17.218	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.198.151.45	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.176.17.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.95	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.89.217.229	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
2.55.25.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.120	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

04-21-2016-11:04:03 to 04-21-2016-12:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
2.53.49.31	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
109.253.204.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
2.55.171.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
17.138.55.96	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.55.96	Block	6
2.55.186.52	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/mobile	Block	5
109.253.220.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.253.220.76	Block	4
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	4
94.188.161.145	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew	Block	4
2.53.63.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.137.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
81.218.56.171	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.56.171	Block	3
2.55.186.52	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 2.55.186.52	Block	3
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	2
46.19.85.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.75.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.226	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
40.77.167.18	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/brothers/gallery/	None	1
2.53.49.31	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	1
91.231.192.149	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
80.246.130.72	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	Block	1
46.19.85.183	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
216.72.40.186	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
176.13.6.119	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.167.25	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.220.76	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2113-he/cogat.aspx	Block	1
176.13.15.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
40.77.167.73	United States	147.237.72.166	aka.idf.il	Unknown Parameter sig2 in aka.idf.il/main/giyus/general.aspx	None	1
2.53.180.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il./giyus	Block	1
81.218.22.216	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
46.19.86.159	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.253.226.108	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/5/71725.pdf¶	Block	1
87.69.59.219	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
2.53.43.83	Israel	147.237.0.19	madim.atal.idf.i	SSL Untraceable Connection - Open Mode	None	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/mainfs.asp	Block	1
207.46.13.18	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/...	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.86.233	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
157.55.39.189	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
37.60.46.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
89.138.118.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.49.105	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/sip_storage/files	Block	1
46.19.85.183	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 46.19.85.183 (Open Mode)	None	1
207.46.13.115	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/2/62532.pdfg2=whvq9jgvov3igm-oflegda	Block	1
81.218.70.243	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 81.218.70.243	Block	1

04-21-2016-11:04:03 to 04-21-2016-12:04:03