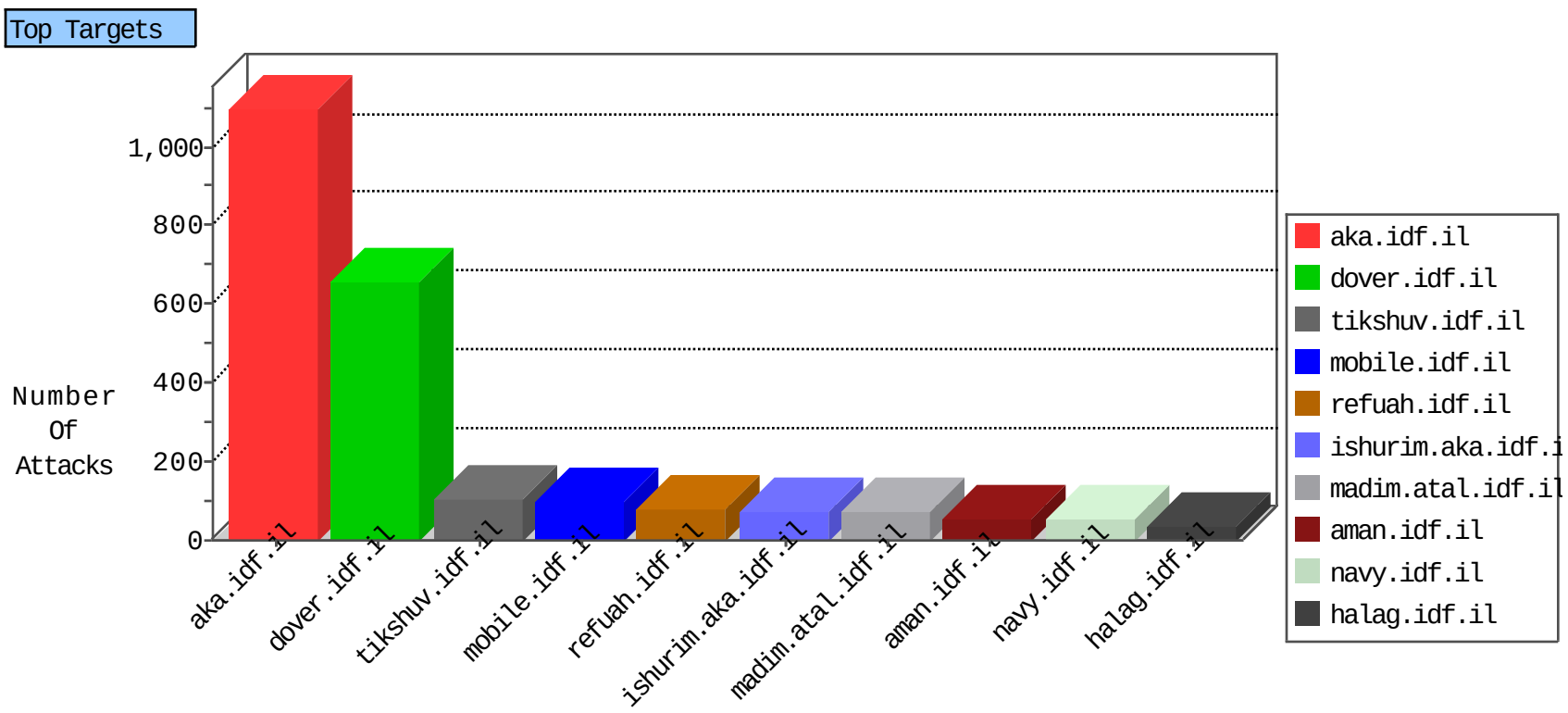
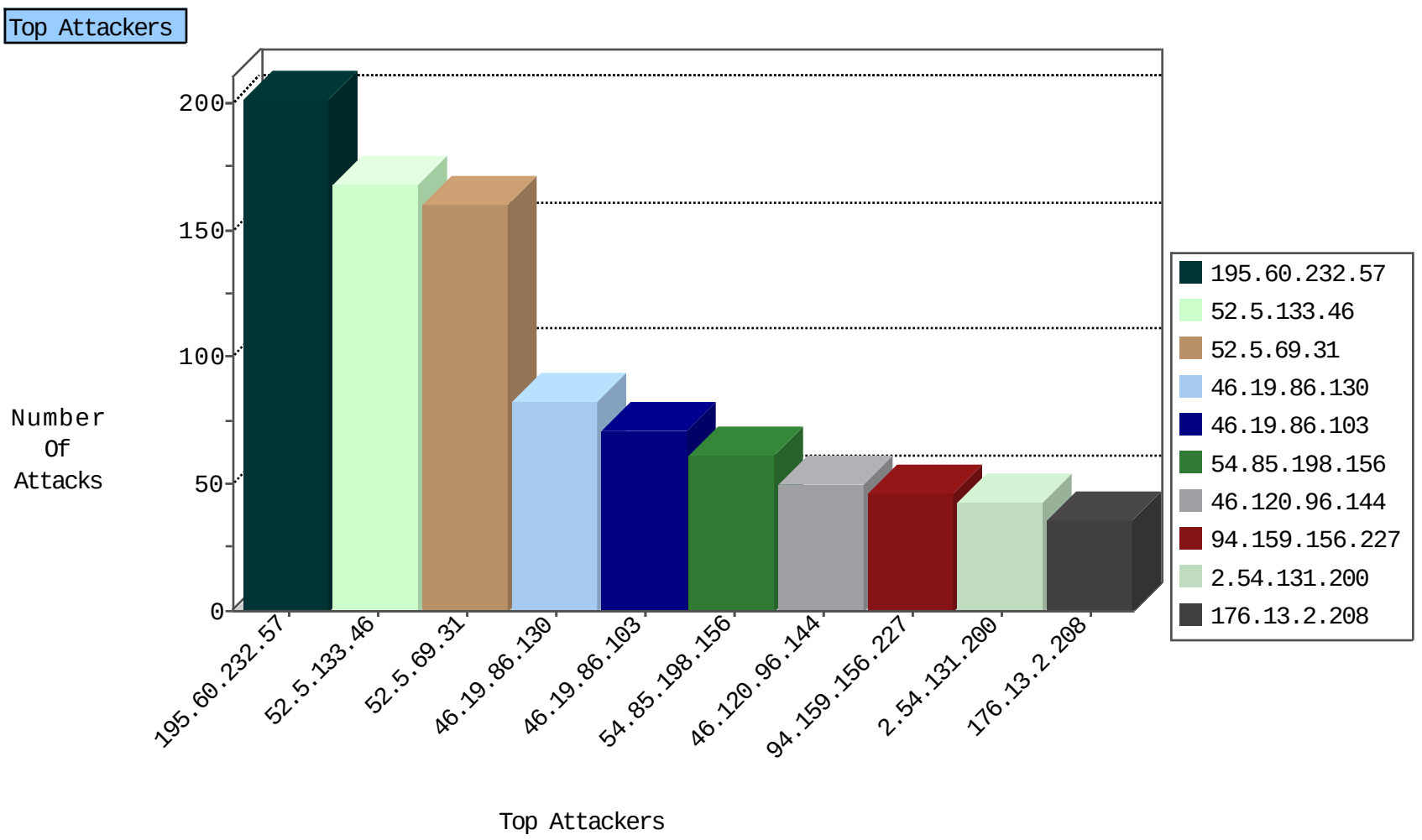
02-15-2016-19:04:06 to 02-15-2016-20:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-15-2016-19:04:06 to 02-15-2016-20:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	23
46.120.96.144	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
93.172.30.60	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
213.8.204.29	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
5.29.158.190	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
185.94.111.1		147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
31.210.186.137	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
185.130.5.224		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
107.150.60.74	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1
185.130.5.201		147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
62.210.84.96	France	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
93.158.203.154	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1

02-15-2016-19:04:06 to 02-15-2016-20:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-15-2016-19:04:06 to 02-15-2016-20:04:06

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
109.67.176.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.108.132.58	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
93.173.15.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.207.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.117	147.237.76.86	Ukraine	navy.idf.il	ET SCAN Potential SSH Scan	1
84.95.209.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.117	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
79.181.223.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.120.151.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.159.33.211	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.120.58.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.85.191	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.92.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.159.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.197.167	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.151.44.117	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.94.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.117	147.237.77.216	Ukraine	dover.idf.il	ET SCAN Potential SSH Scan	1
85.250.30.208	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.117	147.237.76.39	Ukraine	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
82.166.247.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
188.126.77.138	147.237.76.31	Sweden	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.104.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.120.96.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.19.86.214	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
177.238.80.56	147.237.77.176	Mexico	matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.44.134.10	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-15-2016-19:04:06 to 02-15-2016-20:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
52.5.133.46	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	163
52.5.69.31	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	158
46.19.86.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	75
46.19.86.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
195.60.232.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	57
54.85.198.156	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	57
195.60.232.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	55
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
82.80.49.25	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
46.120.96.144	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
5.29.106.173	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
195.60.232.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	28
79.179.106.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
194.90.134.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
85.65.151.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
77.126.12.205	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
149.78.234.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
2.52.131.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.120.96.144	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.12.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
77.127.218.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.0.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.65.2.230	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.115.248.2	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.64.218.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.142.181.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.146.244	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
79.181.200.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
185.32.179.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.86.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
185.32.179.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
185.32.179.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
132.185.160.121	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
50.245.115.206	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.64.145.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
109.64.145.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
188.120.148.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.207	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
87.68.69.252	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
77.126.12.205	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
50.245.115.206	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.54.20.209	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.75	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
2.54.20.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.173.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

02-15-2016-19:04:06 to 02-15-2016-20:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.60.232.57	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 195.60.232.57	Block	49
94.159.156.227	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 94.159.156.227	Block	45
2.54.131.200	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
176.13.2.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
80.246.137.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
185.120.126.49		147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.120.126.49	Block	17
46.19.86.130	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
109.64.98.18	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.64.98.18	Block	7
37.142.64.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	5
80.246.136.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.64.98.18	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	4
81.218.200.96	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1283-he/refuah.aspx/	Block	4
46.19.86.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.142.68.49	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	3
216.35.195.247	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
52.5.133.46	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on aka.idf.il/main/home/default.aspx	Block	2
217.132.91.231	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	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
84.228.67.19	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
193.201.224.170	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/894-he/chinuch.aspx	Block	1
79.178.113.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.28	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/form.asp	Block	1
52.5.69.31	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on aka.idf.il/main/home/default.aspx	Block	1
5.29.1.18	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
94.159.156.227	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
82.80.49.25	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
185.27.106.23	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
37.142.156.225	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
109.64.131.213	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
85.65.100.8	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.54.164.209	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
79.181.200.159	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/giyus/qanda/default.asp	None	1
5.29.106.173	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
216.35.195.247	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp in www.aka.idf.il/main/giyus/general.aspx	None	1
84.111.232.201	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$117 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
109.65.167.243	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 109.65.167.243 (Unknown SSL Session)	None	1
46.19.85.75	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
85.65.234.148	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
2.54.174.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	Block	1
195.60.232.57	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/3390.png	Block	1
176.13.0.220	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$6 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
54.85.198.156	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on aka.idf.il/main/home/default.aspx	Block	1
84.228.42.6	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/sachar/mas.aspx	Block	1
77.127.63.39	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
185.120.126.49		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/[object object]	Block	1
109.65.167.243	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
87.69.170.249	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1

02-15-2016-19:04:06 to 02-15-2016-20:04:06