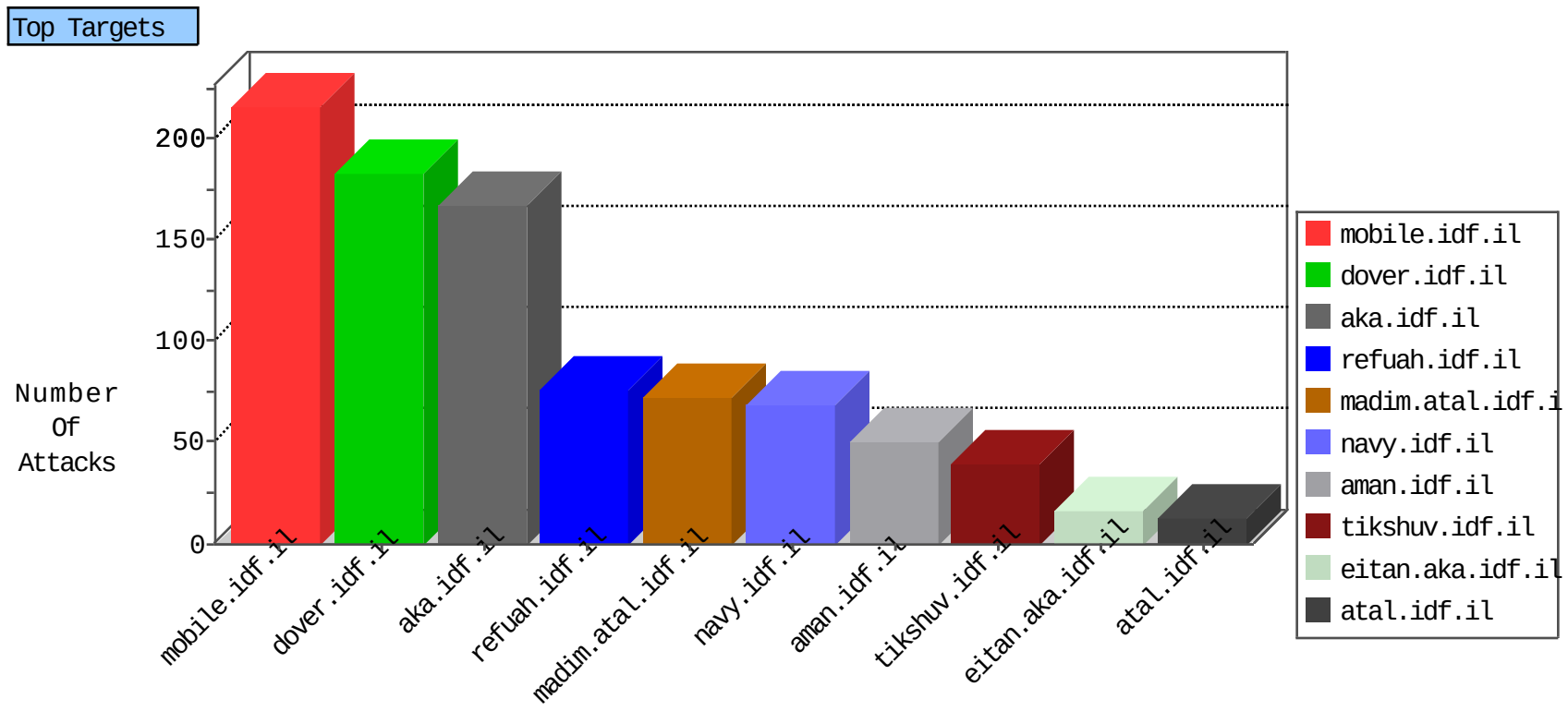
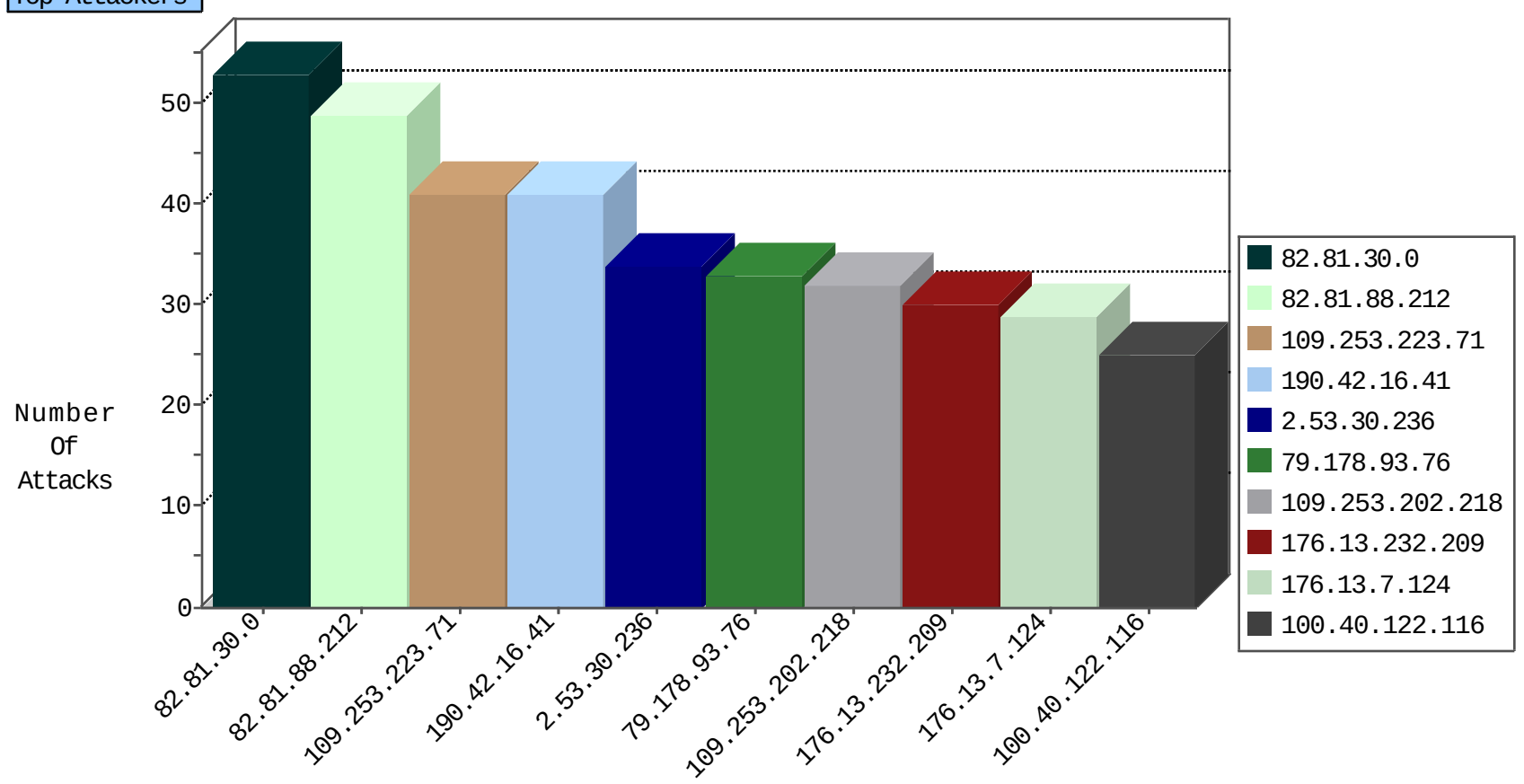
08-31-2016-22:04:07 to 08-31-2016-23:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-31-2016-22:04:07 to 08-31-2016-23:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
77.126.67.134	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
91.230.107.174	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
66.240.192.138	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1
71.6.165.200	United States	147.237.76.177	ncore.idf.il	Black List	drop	1

08-31-2016-22:04:07 to 08-31-2016-23:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-31-2016-22:04:07 to 08-31-2016-23:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.76.200	Israel	eitan.aka.idf.il	Xenu Link Sleuth User Agent	2
64.72.96.150	147.237.0.15	United States	kosher-kravi.idf.il	Admin login page scan - Havij	1
194.58.37.44	147.237.77.74	Russian Federation	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
61.240.144.65	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
193.201.225.149	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 1024	1
58.65.240.98	147.237.77.227	Indonesia	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.200.120	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
58.65.240.98	147.237.76.30	Indonesia	himush.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.200.120	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -sS window 2048	1
66.249.64.230	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
64.72.96.150	147.237.76.147	United States	chinuch.aka.idf.il	Admin login page scan - Havij	1
64.72.96.150	147.237.76.39	United States	mobile.meitav.idf.il	Admin login page scan - Havij	1
61.240.144.65	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
193.201.225.149	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
193.201.225.149	147.237.8.27	Ukraine	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
58.65.240.98	147.237.76.31	Indonesia	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.200.120	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -sS window 3072	1
5.255.90.133	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -f -sS	1
64.72.96.150	147.237.77.216	United States	dover.idf.il	Admin login page scan - Havij	1
64.72.96.150	147.237.76.86	United States	navy.idf.il	Admin login page scan - Havij	1

08-31-2016-22:04:07 to 08-31-2016-23:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.81.88.212	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	48
109.253.223.71	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
176.13.7.124	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.178.93.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
141.0.13.169	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
109.67.144.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.86.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.178.93.76	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	14
80.246.137.95	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
190.42.16.41	Peru	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
46.19.86.88	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.149.229	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.28.156.98	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.81.30.0	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	11
82.81.30.0	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
82.81.30.0	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.86.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
82.81.30.0	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack		monitor	8
37.26.148.158	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
109.253.206.177	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
5.102.195.217	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
2.53.30.236	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
37.26.148.158	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
100.40.122.116	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	7
82.81.30.0	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
100.40.122.116	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.53.30.236	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
176.13.232.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
100.40.122.116	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
190.42.16.41	Peru	147.237.77.216	dover.idf.il	SYN Attack		monitor	6
109.253.206.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.30.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.4.119	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.242.224.133	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.232.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.168.104.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
89.139.151.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
176.13.232.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.168.104.198	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
190.42.16.41	Peru	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
107.181.69.225	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
2.53.30.236	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	5
176.13.232.209	Israel	147.237.72.166	aka.idf.il	SYN Attack		monitor	5
109.253.243.36	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
190.42.16.41	Peru	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
100.40.122.116	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
91.135.104.252	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
190.42.16.41	Peru	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
46.116.43.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
176.13.229.93	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4

08-31-2016-22:04:07 to 08-31-2016-23:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.202.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
84.110.177.147	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	11
46.19.85.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
109.253.223.71	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
109.253.212.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
176.13.243.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.26.147.163	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	5
176.13.7.124	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
46.19.86.205	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.67.144.45	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
192.117.10.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.4.119	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.88	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.229	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.178.184.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.28.156.98	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.206.64	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.228.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.117.10.226	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1
64.72.96.150	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Malformed URL	Block	1
84.111.21.108	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
77.138.71.79	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
213.169.41.88	Bulgaria	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.192	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/8/112228.pdf	Block	1
79.177.148.126	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.64	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/about_our_courses.asp	Block	1
64.72.96.150	United States	147.237.0.34	tikshuv.idf.il	Malformed URL http/1.1	Block	1
148.251.13.51	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
86.173.160.186	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
2.53.30.236	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.138.84.182	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
180.97.106.37	China	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.64.251	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	1
37.26.147.163	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.120	United States	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 207.46.13.120	Block	1
64.72.96.150	United States	147.237.76.86	navy.idf.il	Multiple Malformed URL from 64.72.96.150	Block	1
87.204.52.13	Poland	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
77.138.203.37	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
180.97.106.161	China	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
46.120.122.219	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/	None	1
82.81.88.212	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
77.126.47.138	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

08-31-2016-22:04:07 to 08-31-2016-23:04:07