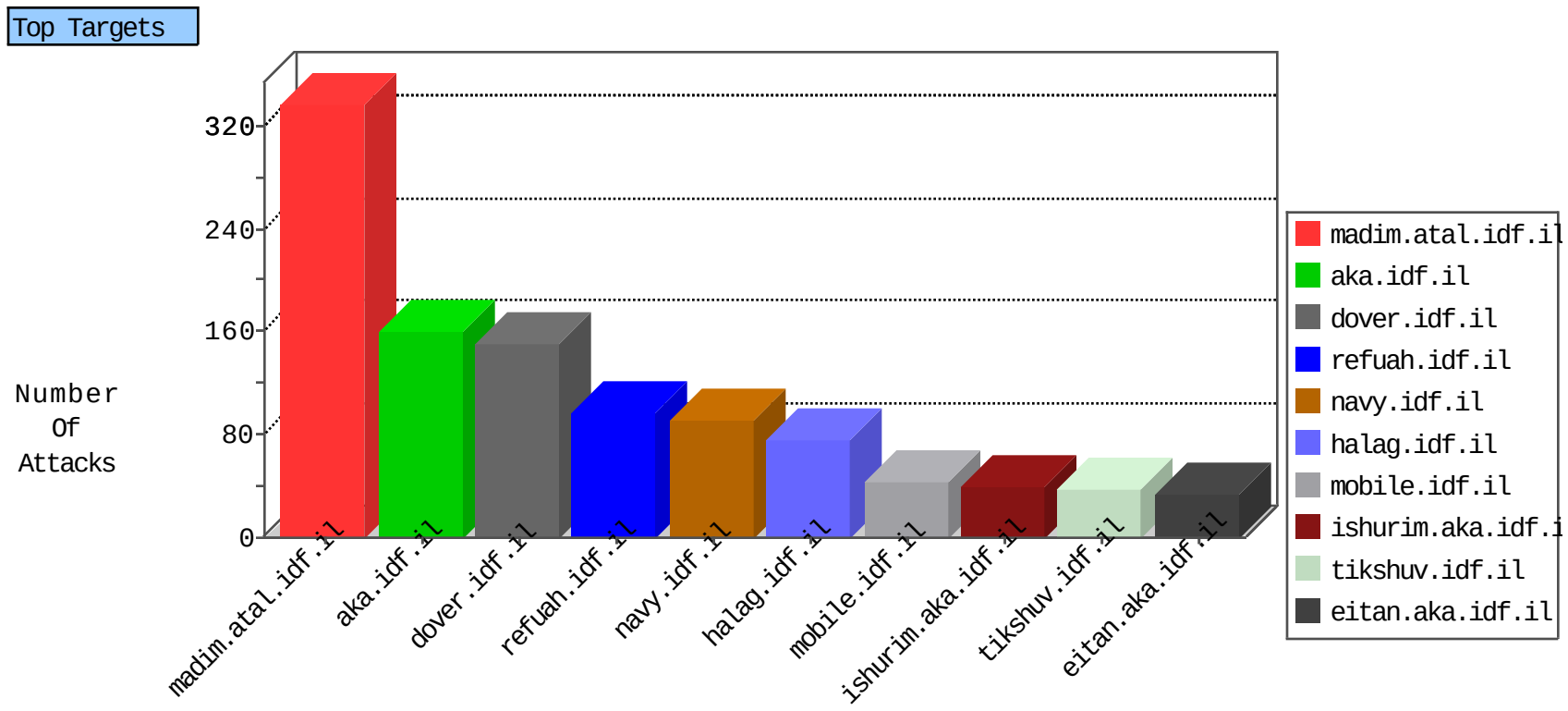
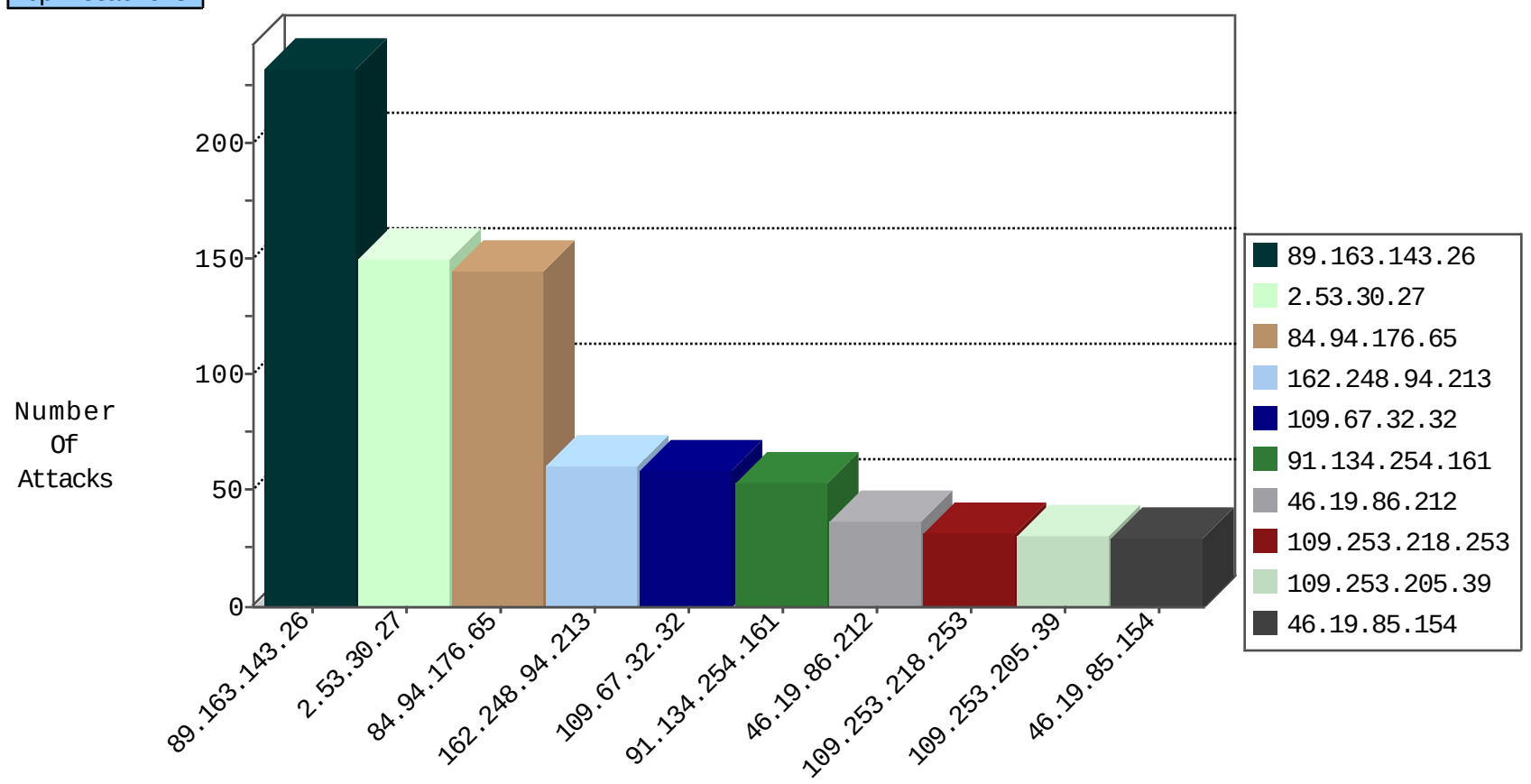
09-06-2016-20:04:00 to 09-06-2016-21:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-06-2016-20:04:00 to 09-06-2016-21:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
190.82.85.70	Chile	147.237.8.27	e.madim.atal.idf.il	L4 Source or Dest Port Zero	drop	3
71.6.167.142	United States	147.237.76.177	ncore.idf.il	Black List	drop	1

09-06-2016-20:04:00 to 09-06-2016-21:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.130	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-06-2016-20:04:00 to 09-06-2016-21:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
173.196.183.198	147.237.77.216	United States	dover.idf.il	Xenu Link Sleuth User Agent	2
5.255.90.133	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.120.19	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	1
93.158.203.195	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
89.216.119.94	147.237.76.42		refuah.idf.il	ET SCAN NMAP -sS window 2048	1
85.105.166.24	147.237.77.216	Turkey	dover.idf.il	ET SCAN NMAP -sS window 3072	1
77.127.0.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.195	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.236.120.253	147.237.72.166	Russian Federation	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
89.216.119.94	147.237.76.42		refuah.idf.il	ET SCAN NMAP -f -sS	1
85.105.166.24	147.237.77.216	Turkey	dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -sS window 1024	1

09-06-2016-20:04:00 to 09-06-2016-21:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
109.67.32.32	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	58
109.67.174.226	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
89.163.143.26	Germany	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
46.19.85.154	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
89.163.143.26	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
89.163.143.26	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
89.163.143.26	Germany	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
89.163.143.26	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
89.163.143.26	Germany	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
89.163.143.26	Germany	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
89.163.143.26	Germany	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
117.216.35.12	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
162.248.94.213	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	16
162.248.94.213	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
162.248.94.213	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	15
46.19.86.212	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
79.183.49.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.116.124.70	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
162.248.94.213	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
109.253.218.253	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.86.212	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.212	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
109.253.218.253	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	8
109.253.218.253	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
109.253.218.253	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
79.176.33.146	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.51	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
91.134.254.161	Bulgaria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
87.69.208.55	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
37.26.146.206	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.51	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
77.126.20.243	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
185.3.147.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
91.134.254.161	Bulgaria	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
109.253.204.164	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
91.134.254.161	Bulgaria	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
173.165.81.51	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
91.134.254.161	Bulgaria	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.212	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
31.154.81.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	4
46.19.86.146	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
141.226.217.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.146	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.186.75.173	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
212.199.95.73	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.3.147.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.134.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.30.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	150
84.94.176.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	145
109.253.205.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
79.178.46.212	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 79.178.46.212	Block	26
213.57.105.224	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	5
213.57.59.50	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 213.57.59.50 (Open Mode)	None	4
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
173.165.81.51	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
77.139.78.98	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
77.139.78.98	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
2.55.161.136	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	2
5.28.190.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	2
50.202.143.214	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.42	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in madim.atal.idf.il/1088-he/meretz.aspx	Block	2
5.228.186.28	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
180.76.15.162	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9700-he/refuah.aspx	Block	1
54.158.62.102	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
46.19.86.146	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
95.86.123.40	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	1
79.177.146.219	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
213.57.233.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.116.124.70	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
109.253.204.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.108.14.8	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
37.26.147.194	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
192.203.40.251	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/megurim/	Block	1
46.19.86.216	Israel	147.237.77.233	atal.idf.il	Illegal HTTP Version	Block	1
107.77.104.26	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
2.55.3.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
46.242.92.0	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
84.108.241.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.142.5.170	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
77.139.121.241	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
201.211.191.110	Venezuela	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/assetlinks.json	Block	1
46.19.86.216	Israel	147.237.77.233	atal.idf.il	Malformed URL http/1.1	Block	1
109.66.172.192	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
79.178.46.212	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/0/2890.pd	Block	1
77.138.115.170	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
157.55.39.115	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp/	Block	1
50.202.143.214	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
85.64.50.90	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.244	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
77.139.173.10	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.249.66.146	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
46.19.86.216	Israel	147.237.77.233	atal.idf.il	Unknown HTTP Request Method ade2.png in URL www.atal.idf.ilhttp/1.1	Block	1
109.67.32.32	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.183.49.81	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1