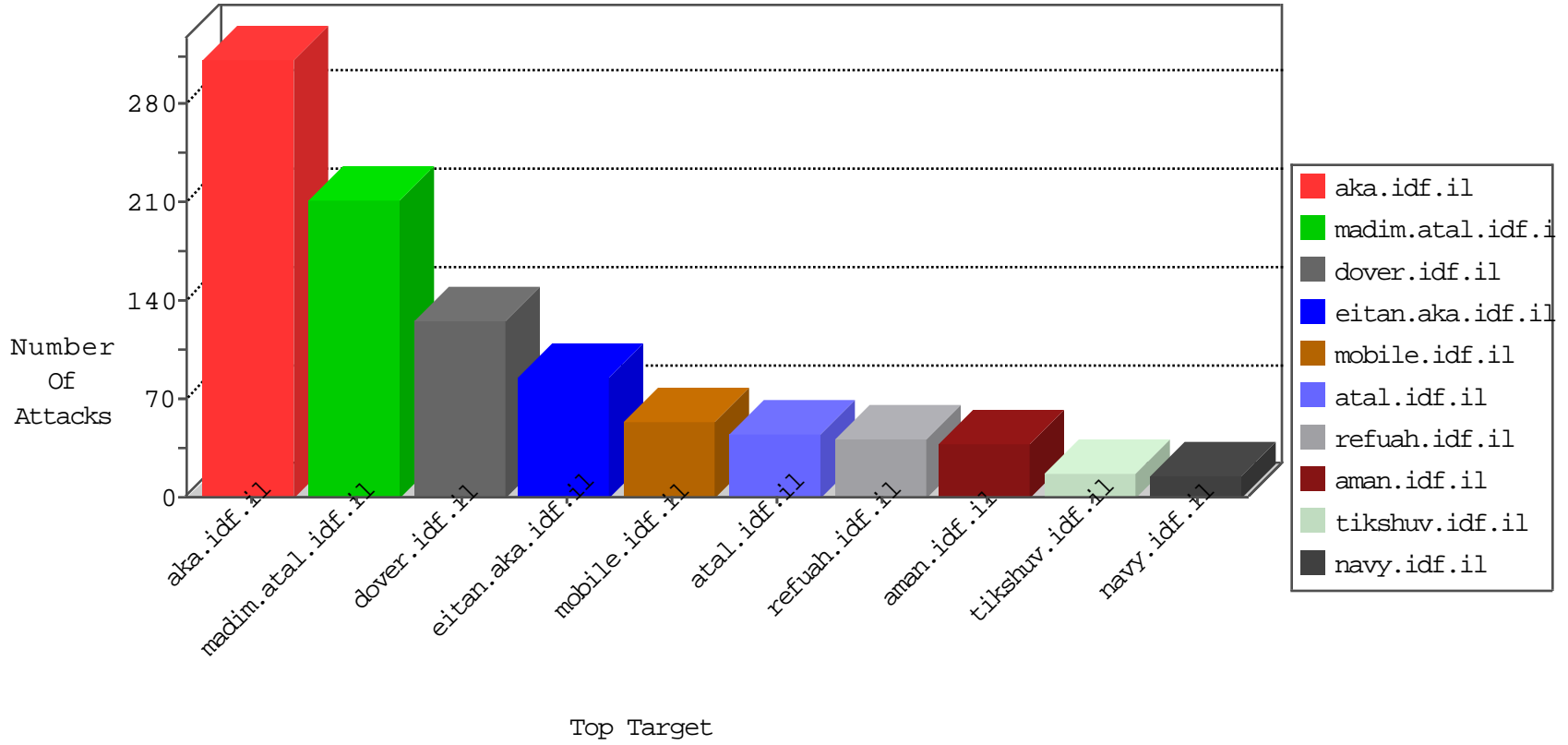


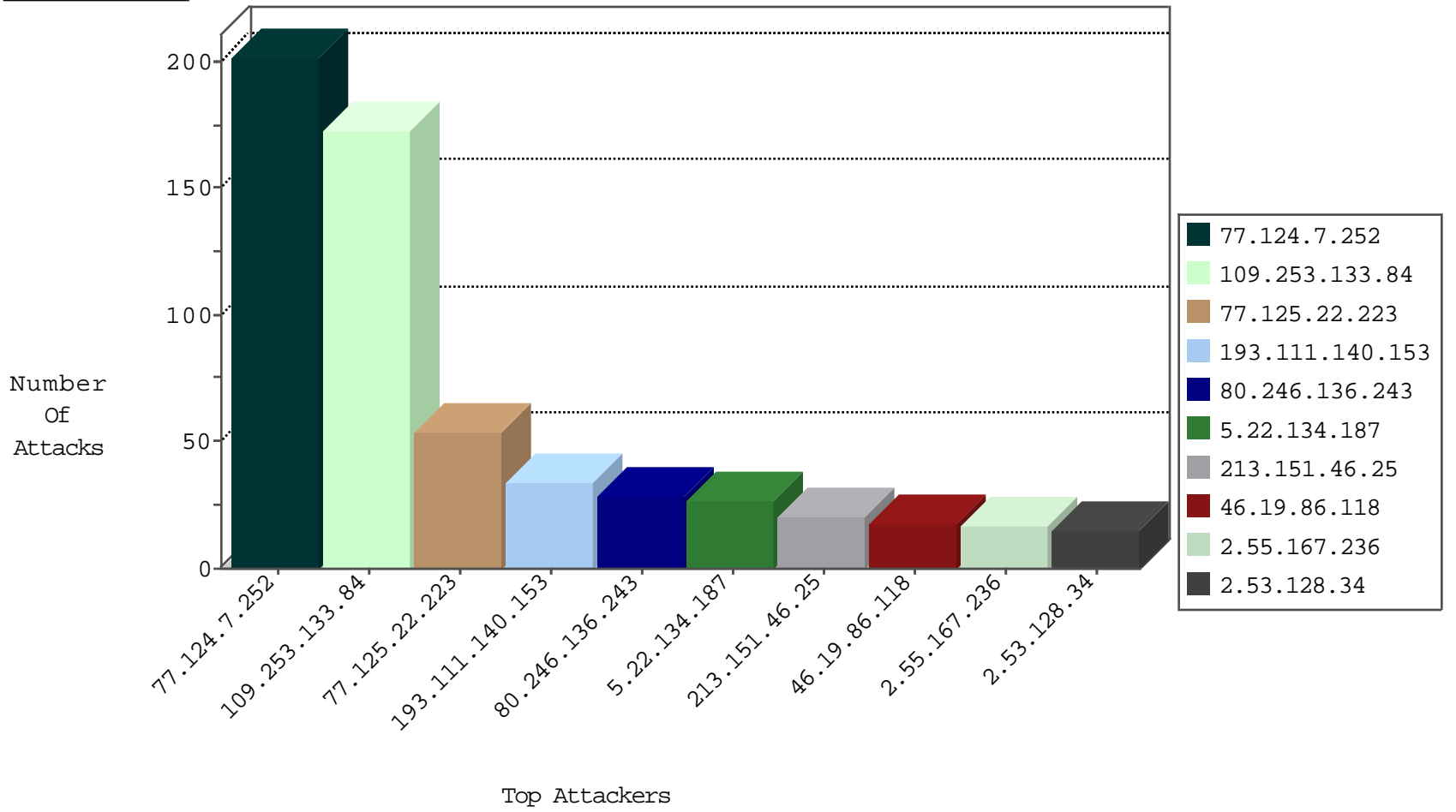
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.124.7.252	Israel	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	8270
77.124.7.252	Israel	147.237.72.166	aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1798
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
137.132.80.110	Singapore	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
82.81.90.7	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
46.45.137.72	Turkey	147.237.76.176	test.ncore.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.68	Switzerland	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
193.111.140.153	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	20
193.111.140.153	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	10
193.111.140.153	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	4

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
77.124.7.252	147.237.72.166	Israel	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	15
77.124.7.252	147.237.72.166	Israel	aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	10
212.199.57.192	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	7
109.64.55.1	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	5
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
77.124.7.252	147.237.72.166	Israel	aka.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
133.242.4.52	147.237.76.197	Japan	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
133.208.21.66	147.237.72.166	Japan	aka.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
212.116.72.226	147.237.8.14	Sweden	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
109.60.153.178	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
40.121.139.43	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
212.116.72.226	147.237.8.14	Sweden	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
93.158.203.168	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.77.61	United States	e.cogat.idf.il	ET DROP Dshield Block Listed Source	1
91.224.160.106	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.162	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.33	Netherlands	idf.il	ET SCAN Potential SSH Scan	1
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
91.224.160.106	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
133.242.4.52	147.237.8.46	Japan	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.130.195	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
133.208.21.66	147.237.72.156	Japan	aman.idf.il	ET SCAN NMAP -sS window 1024	1
46.20.217.130	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	1
212.116.72.226	147.237.8.14	Sweden	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
109.60.153.178	147.237.0.33	Russian Federation	idf.il	ET SCAN NMAP -sS window 1024	1
212.25.122.65	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
93.158.203.168	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
186.60.139.129	147.237.76.31	Argentina	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.224.160.106	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.162	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.125.22.223	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
5.22.134.187	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
213.151.46.25	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
2.53.128.34	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
87.69.52.140	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
185.32.179.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.60.44.121	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.86.118	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
176.13.2.196	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
116.202.36.105	India	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
77.125.59.127	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
109.253.133.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.146.114.66	Georgia	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.135.146	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.124.7.252	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
5.29.145.8	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.153	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.55.167.236	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
2.55.167.236	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.55.167.236	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
31.175.234.125	Poland	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.86.118	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
176.13.2.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
31.175.234.125	Poland	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.195.210	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	4
185.62.121.12	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
31.175.234.125	Poland	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
185.62.121.1	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
5.22.134.187	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
37.46.41.19	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	3
188.161.112.5	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
141.226.162.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.178.237.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
185.120.124.83	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
69.242.30.107	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.223	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
84.108.136.134	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
80.246.133.122	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.10.232	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.55.167.236	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
66.212.179.106	Canada	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
84.109.209.137	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.133.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	166
80.246.136.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
46.19.85.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.246.137.240	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
85.64.150.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.118	Israel	147.237.76.42	refuah.idf.il	Distributed Unknown HTTP Request Method	Block	2
109.253.199.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.25.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.200.53	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/gyus/yahash/sheelon.aspx	Block	2
213.8.204.19	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
2.53.189.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.118	Israel	147.237.76.42	refuah.idf.il	Distributed Malformed URL	Block	2
213.151.43.13	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/https://mobile.idf.il/	Block	1
46.117.156.132	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/site/templates/controller.asp	Block	1
31.154.81.70	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https://www.aman.idf.il/	Block	1
109.253.133.84	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
208.80.155.222	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/general.aspx	Block	1
109.63.140.189	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Unauthorized Method POST for www.chinuch.aka.idf.il/894-he/chinuch.aspx	None	1
68.180.229.223	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/gyus/general.aspx	Block	1
217.132.86.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.60.44.121	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-7972-he/eitan.	Block	1
84.108.132.104	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
66.249.66.162	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/assetlinks.json	Block	1
212.199.156.81	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/gyus/	Block	1
46.19.86.141	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.67.200.247	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/login.aspx	Block	1
144.82.240.255	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.76.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/assetlinks.json	Block	1
46.116.209.20	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
109.67.224.137	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
80.246.130.0	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/1319-he/refuah.aspx	Block	1
66.102.9.2	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
157.55.39.25	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/ - ٤ ½ - ٤ ½	Block	1
46.19.85.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.250.128.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.76.104	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/apple-app-site-association	Block	1
213.151.43.13	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.151.43.13	Block	1
46.117.156.132	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ...l&sideScroll in www.aka.idf.il/gyus/kadatz/	None	1
5.22.134.187	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.64.181	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
188.120.154.65	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
104.128.144.131	Canada	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/redirect.php	Block	1
67.188.105.121	United States	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1