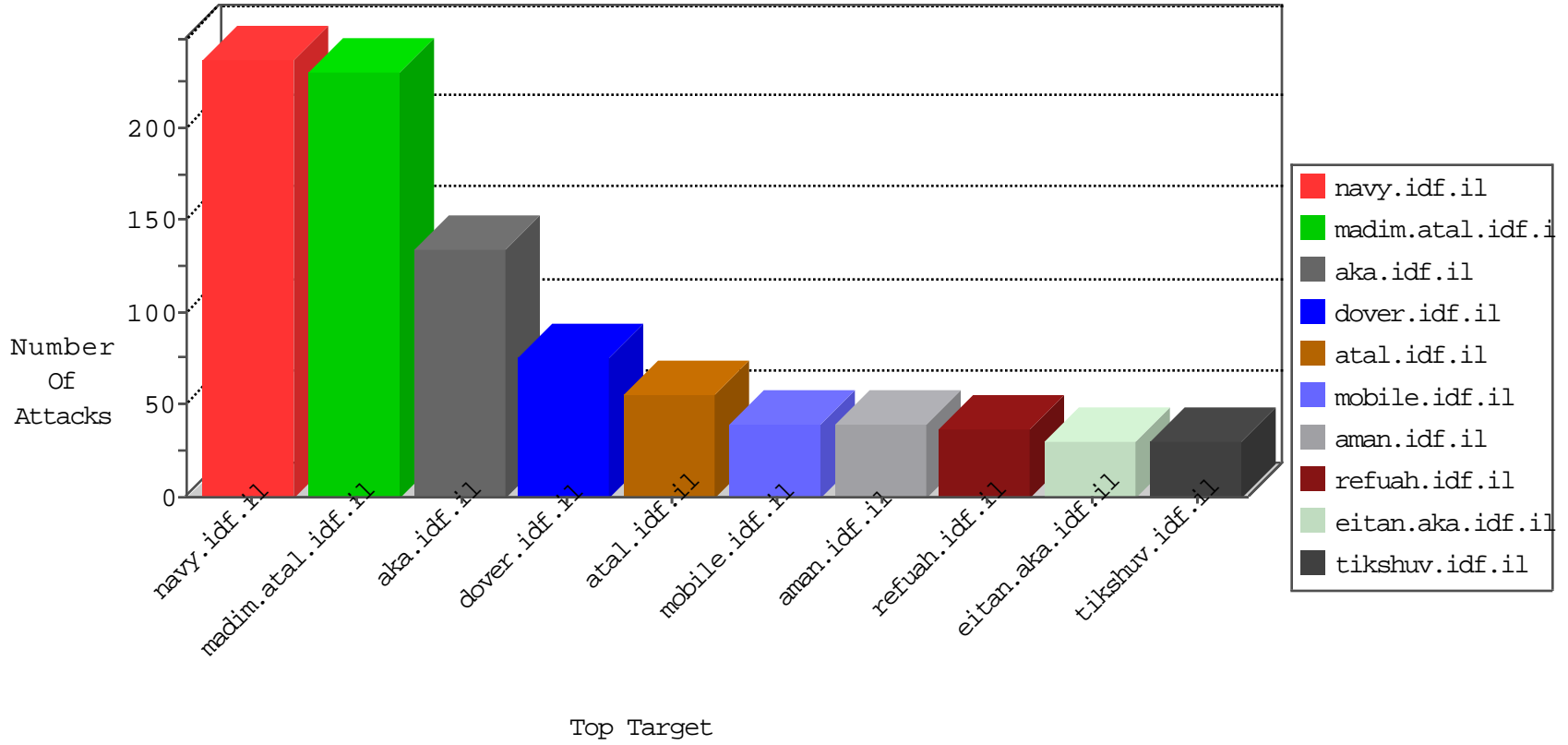


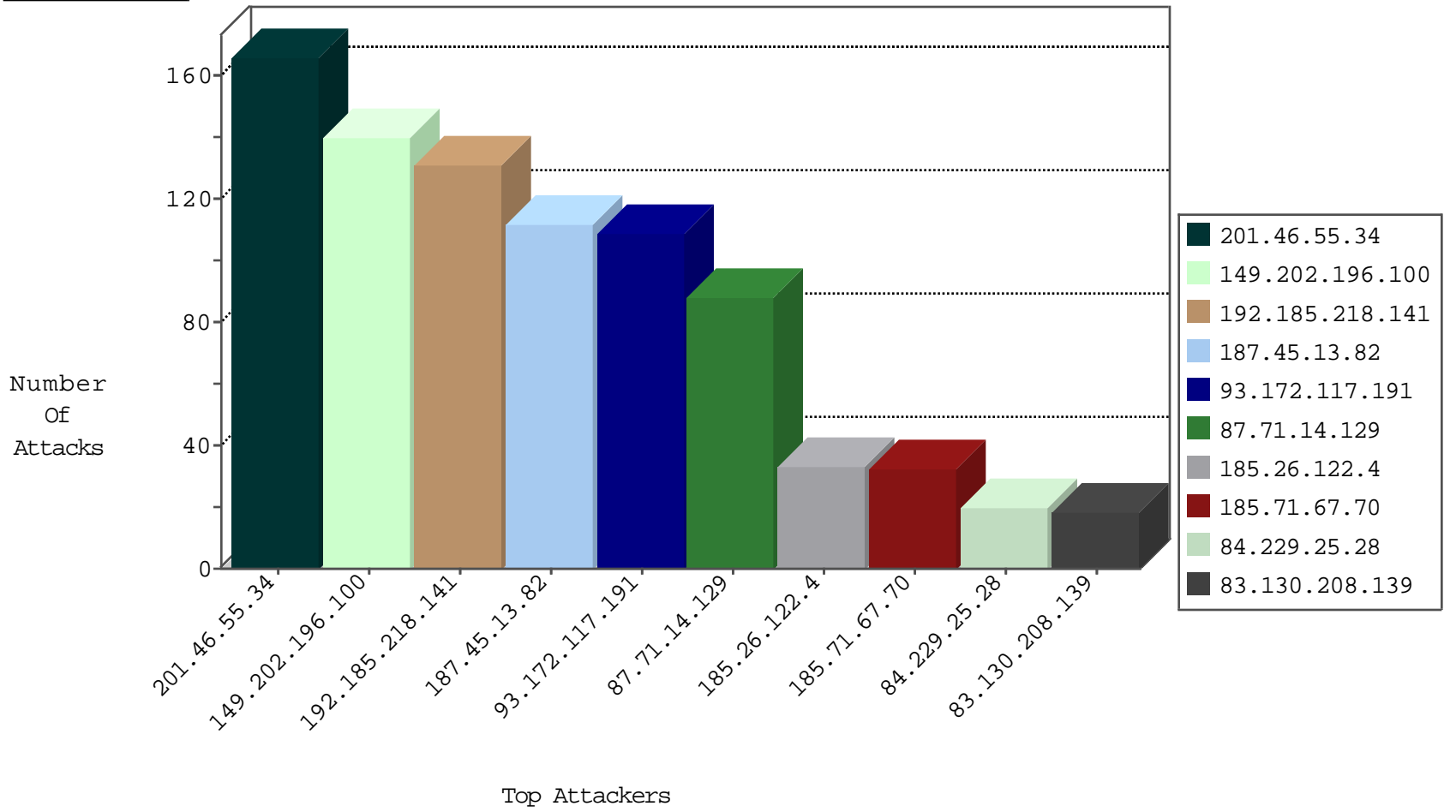
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.59.59.52	China	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
80.82.70.230	Netherlands	147.237.76.44	e.refuah.idf.il	Black List	drop	1
80.82.70.230	Netherlands	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
50.77.136.81	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
69.30.198.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
179.43.141.208	Switzerland	147.237.76.39	mobile.meitav.idf.il	34161: ICMP: Communication with Destination Host is Administratively Prohibited (Code 10)	Block	1
179.43.141.208	Switzerland	147.237.76.42	refuah.idf.il	34161: ICMP: Communication with Destination Host is Administratively Prohibited (Code 10)	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
83.130.208.139	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	9
50.77.136.81	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
218.87.109.253	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
104.237.146.151	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.87.109.253	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
77.124.45.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.227.67.158	147.237.0.19	Sweden	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
200.58.214.138	147.237.76.197	Colombia	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
193.201.225.149	147.237.76.148	Ukraine	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
189.230.1.230	147.237.0.33	Mexico	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.87.109.253	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
142.54.191.210	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
218.87.109.253	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
142.54.191.210	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
218.87.109.253	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
123.176.80.201	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.0.16	China	ny-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
201.38.68.132	147.237.77.243	Brazil	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
23.92.20.154	147.237.0.16	United States	ny-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
200.58.214.138	147.237.76.197	Colombia	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.149	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.72.156	United Kingdom	aman.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
142.54.191.210	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
218.87.109.253	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
139.162.160.132	147.237.0.33	United States	idf.il	ET SCAN Potential VNC Scan 5900-5920	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.202.196.100	France	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	140
185.26.122.4	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	33
185.71.67.70	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	32
46.19.85.156	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
84.229.25.28	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
84.229.25.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
201.46.55.34	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
192.185.218.141	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
201.46.55.34	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
2.53.54.218	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
201.46.55.34	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
201.46.55.34	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
187.45.13.82	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
201.46.55.34	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
192.185.218.141	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.34	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.34	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
187.45.13.82	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
83.130.208.139	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
201.46.55.34	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.34	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
187.45.13.82	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
192.185.218.141	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
187.45.13.82	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
187.45.13.82	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
192.185.218.141	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
201.46.55.34	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
187.45.13.82	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
192.185.218.141	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
188.72.103.227	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
187.45.13.82	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
192.185.218.141	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.34	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.34	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.34	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
192.185.218.141	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
192.185.218.141	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.34	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.34	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.34	Brazil	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.34	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.34	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
201.46.55.34	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.121.82.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
201.46.55.34	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
187.45.13.82	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
37.26.149.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
84.108.132.117	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
192.185.218.141	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
192.185.218.141	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.172.117.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	109
87.71.14.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	88
109.64.10.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.53.34.32	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	4
5.102.195.231	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation asperrorpath in www.idf.il/error.htm	Block	3
77.138.26.190	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	2
77.138.81.248	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	2
2.53.54.218	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.144.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.22.134.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.245.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.31.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.67.124.81	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
79.176.82.230	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
66.249.64.30	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2297.jpg	Block	1
192.116.94.67	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	1
85.65.170.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.181.216.104	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/2970.jpg	Block	1
77.139.242.57	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.242.57	Block	1
83.130.208.139	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.66.232	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
77.139.242.57	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
157.55.39.74	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/sachar/faq.aspx	None	1
84.111.224.175	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.76.70	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/apple-app-site-association	Block	1
79.176.82.230	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.121.82.102	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
85.64.245.112	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1