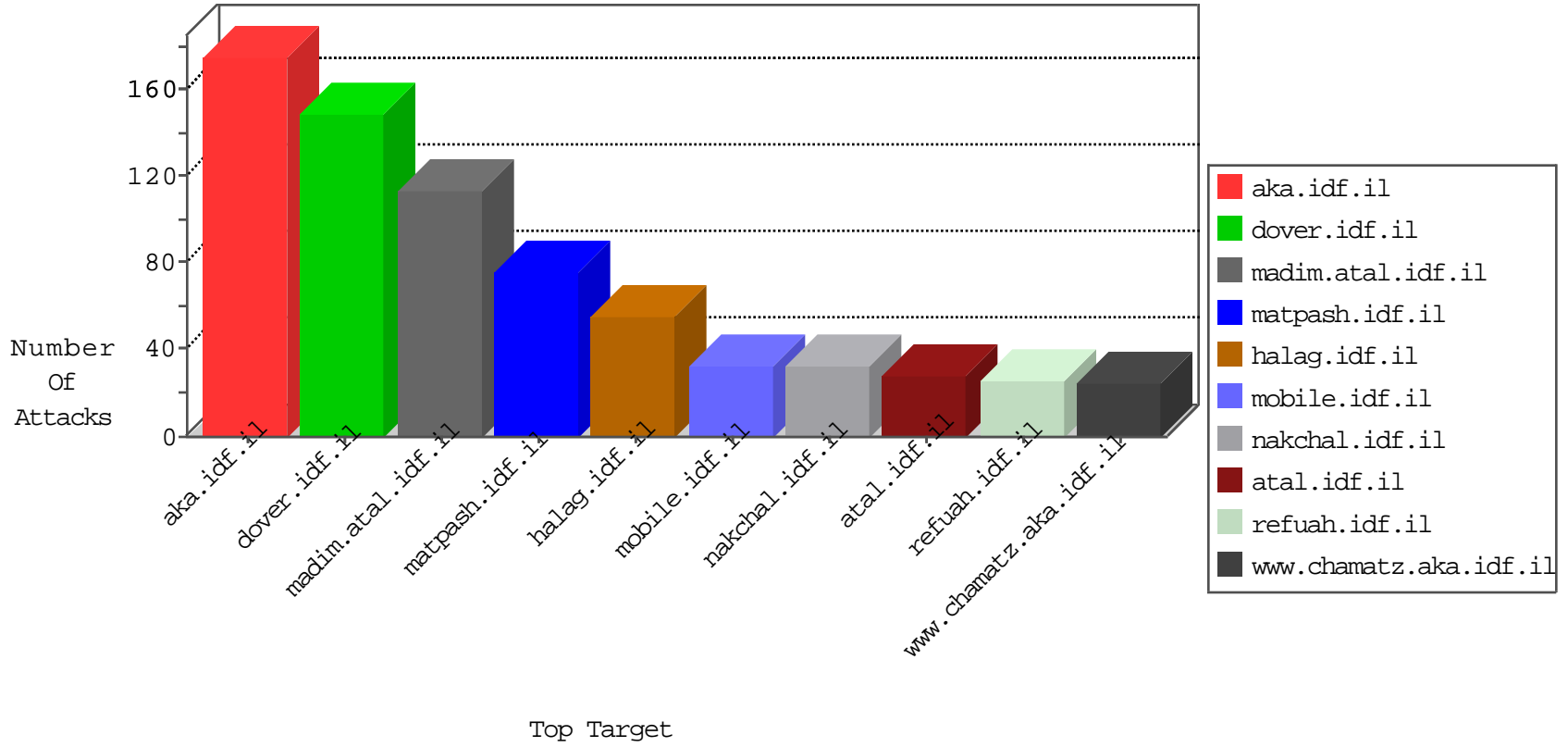


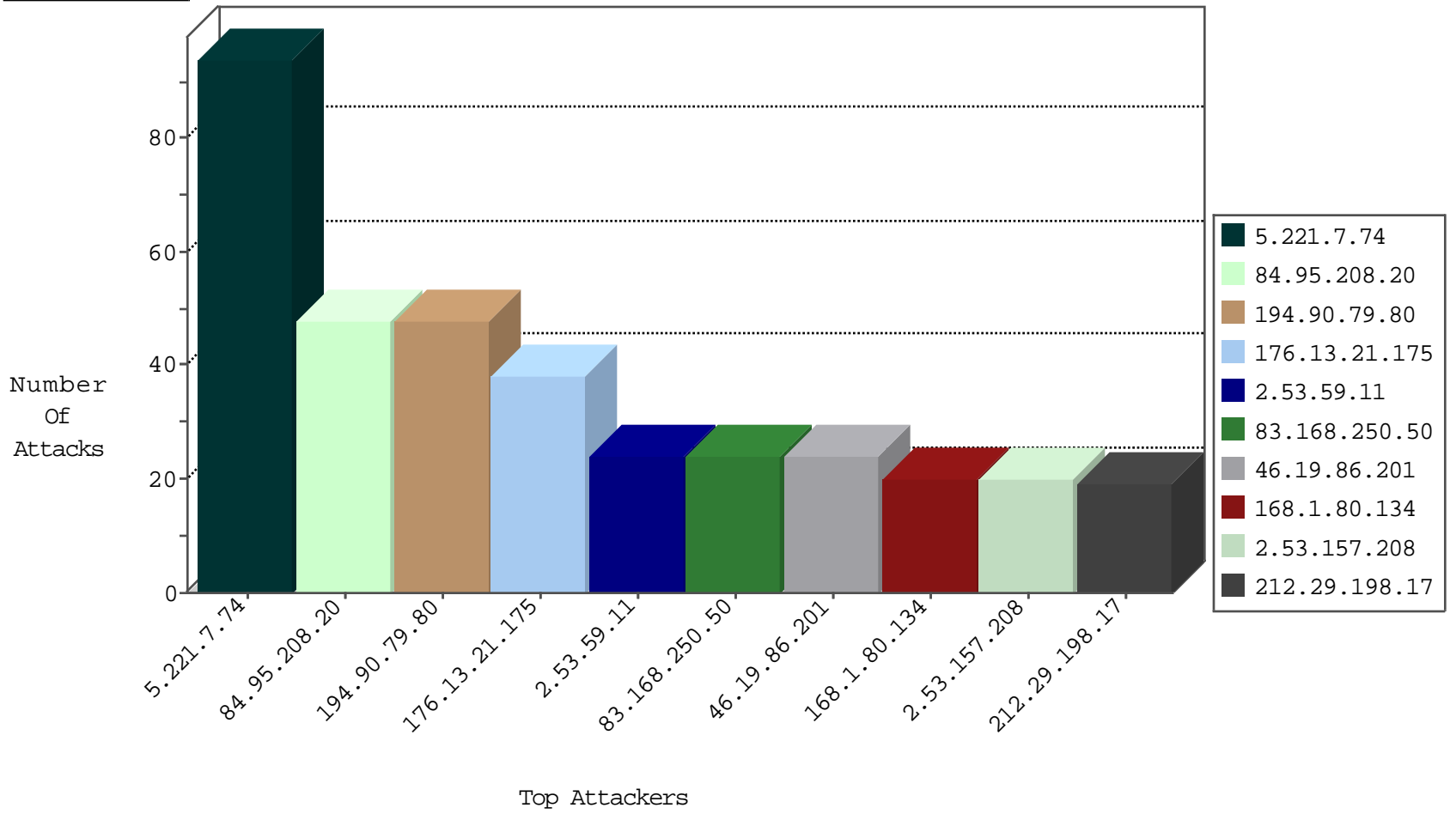
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.244.54	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	19
183.60.48.25	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
5.189.186.243	Germany	147.237.76.197	e.himush.idf.il	Black List	drop	1
91.230.121.156	Ukraine	147.237.76.196	e.sviva.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
114.159.177.231	Japan	147.237.76.196	e.sviva.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
91.230.121.156	Ukraine	147.237.76.148	ggcenter.aka.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.196	e.sviva.idf.il	Black List	drop	1
91.230.121.156	Ukraine	147.237.76.176	test.ncore.idf.il	Black List	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
168.1.80.134	Australia	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.192.134	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
168.1.80.134	147.237.77.233	Australia	atal.idf.il	SQL Injection - Select From	14
192.116.96.192	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
184.168.192.134	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	2
175.142.131.96	147.237.77.216	Malaysia	dover.idf.il	Xenu Link Sleuth User Agent	2
79.176.108.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.138.9.178	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
217.165.67.151	147.237.77.235	United Arab Emirates	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.230	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.210.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.194.176	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
146.185.146.112	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
5.28.137.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
116.12.175.233	147.237.77.216	Singapore	dover.idf.il	ET SCAN NMAP -sS window 1024	1
212.150.10.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.126.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.238.202.219	147.237.0.35	Chile	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1
192.227.171.173	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
80.246.139.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.117.171.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.25.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.226	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
176.13.23.224	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.151.48.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.130	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.179.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.72.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
122.164.174.221	147.237.76.86	India	navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.179.21.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.137.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
192.227.171.173	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
84.92.144.27	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	1
192.227.171.173	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.90.79.80	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	45
5.221.7.74	Iran, Islamic Republic of	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
5.221.7.74	Iran, Islamic Republic of	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	35
83.168.250.50	Sweden	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	24
82.166.93.161	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
5.221.7.74	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
5.221.7.74	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.197	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	12
77.138.51.210	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	9
46.19.85.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
89.139.151.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.86.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.115.200.93	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.106.46.74	Palestinian Territory, Occupied	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
212.29.198.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.157.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
184.168.192.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
2.53.157.208	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
213.151.49.76	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
2.53.157.208	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
2.53.157.208	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.133	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.253.218.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.8.204.23	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.29.198.17	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
82.81.26.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.229.8.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.86.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.81.26.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
192.115.200.93	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
109.253.158.140	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.199.61.93	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.64.228	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.29.198.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
212.29.198.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
5.22.135.133	Israel	147.237.72.166	aka.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
79.181.127.115	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.29.198.17	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
109.253.158.140	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
176.13.5.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.22.125	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.58	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
85.65.11.57	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
157.55.39.175	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
82.81.46.104	Israel	147.237.72.166	aka.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
176.13.21.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
2.53.59.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
46.19.86.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
84.111.152.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
37.26.147.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
46.19.85.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	4
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
2.55.167.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
46.19.86.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
46.19.85.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	3
79.181.127.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
94.153.177.122	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/matash/login/	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
46.19.86.75	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	2
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	2
46.19.85.195	Israel	147.237.76.31	nakchal.idf.il	Abnormally Long Request method	Block	1
80.246.133.77	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/error.png	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
176.13.249.164	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.76.98	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list7.htm	Block	1
66.249.64.78	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	Block	1
46.19.85.195	Israel	147.237.76.31	nakchal.idf.il	Illegal HTTP Version	Block	1
80.246.133.82	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/titlecap.png	Block	1
207.46.13.8	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.76.72	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/assetlinks.json	Block	1
46.19.86.153	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	1
46.19.85.84	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
192.116.96.192	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
77.138.237.146	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/kamlar/faq/default.asp	Block	1
66.249.76.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/apple-app-site-association	Block	1
46.19.85.195	Israel	147.237.76.31	nakchal.idf.il	Malformed URL __atuvs=57c7c55259867c82000	Block	1
80.246.133.174	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.147.213	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
207.46.13.64	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
157.55.39.71	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/piwik.php	Block	1