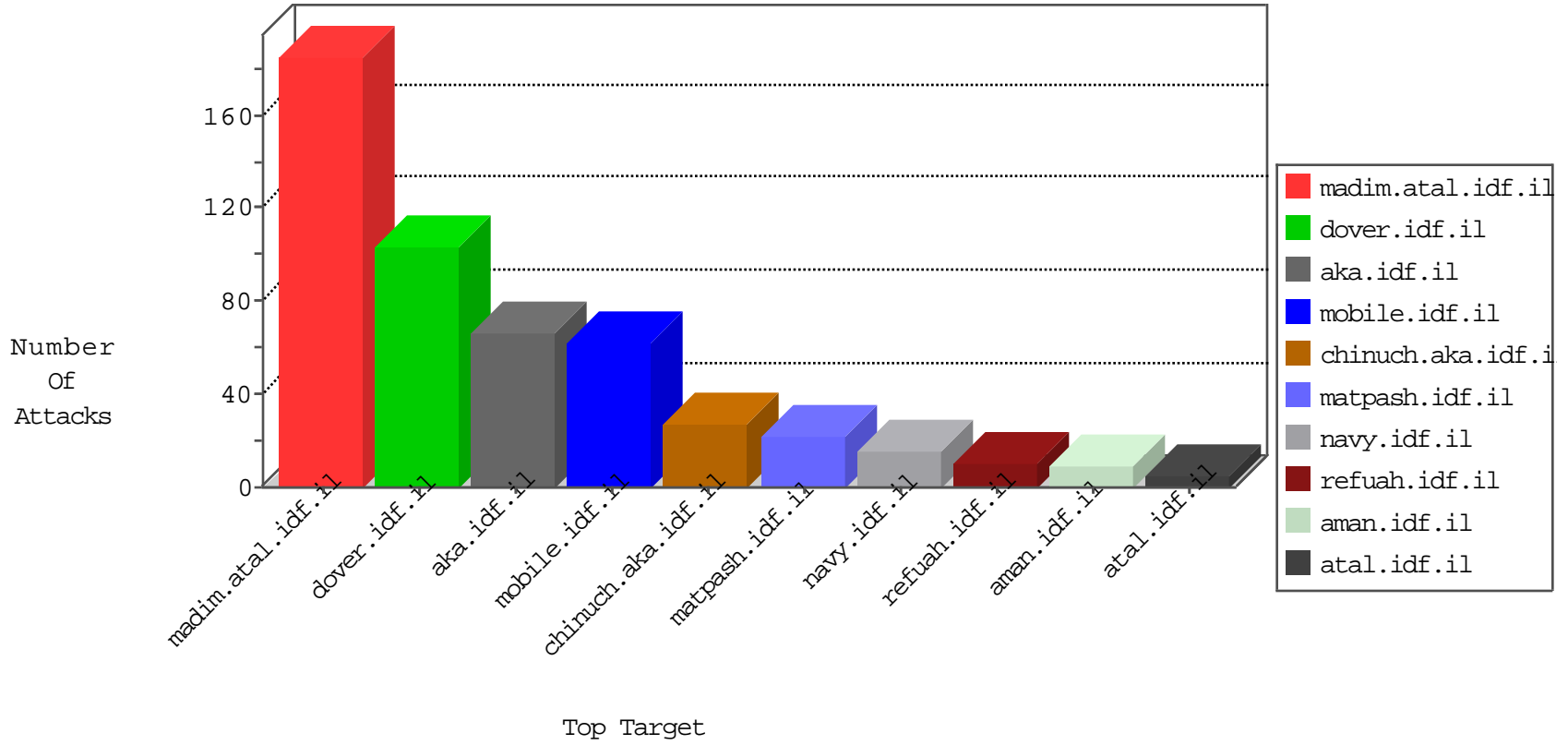


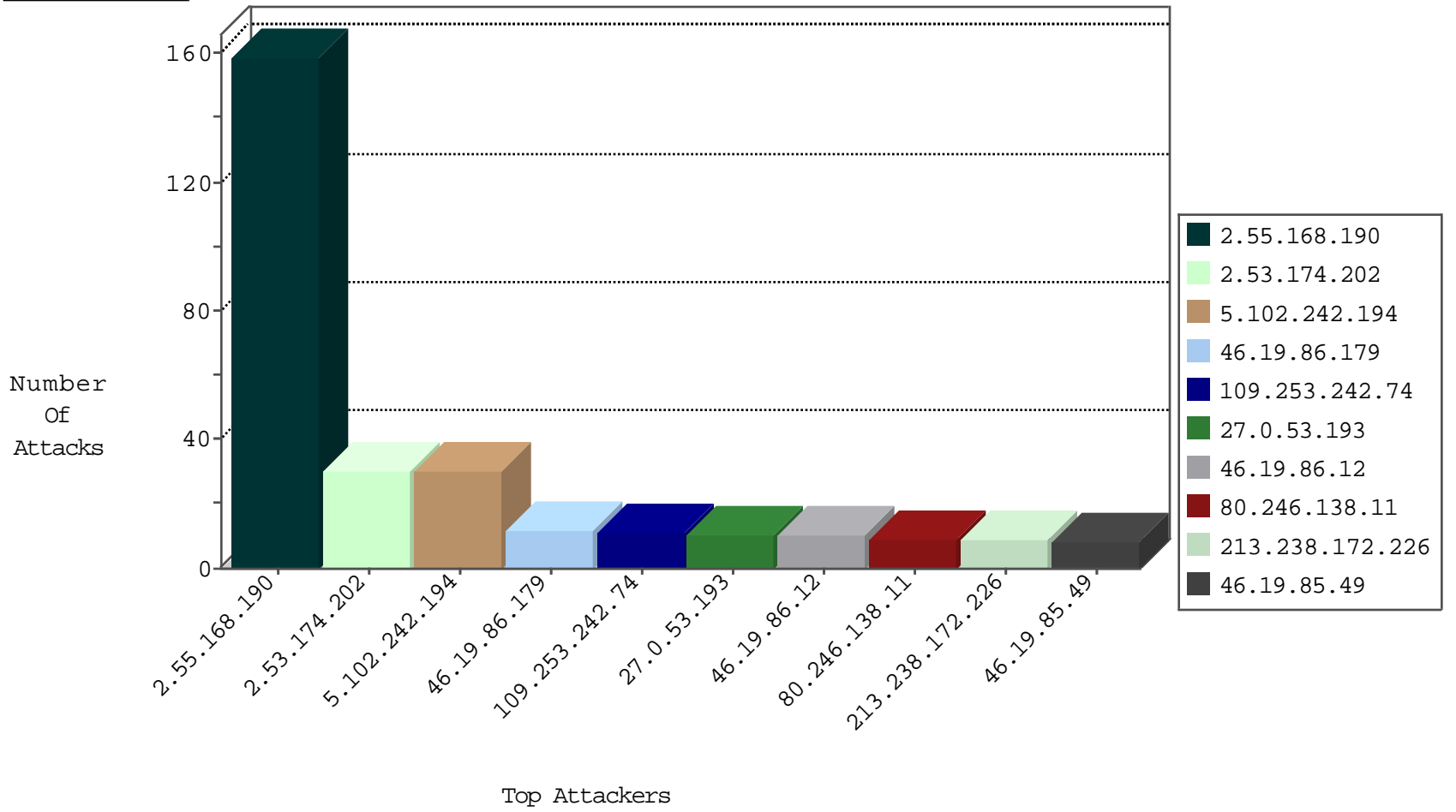
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.204.224.235	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-trafl	forward	2
198.204.224.235	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-trafl	forward	2
69.30.193.250	United States	147.237.76.30	himush.idf.il	block-sp-trafl	forward	2
198.204.224.234	United States	147.237.76.31	nakchal.idf.il	block-sp-trafl	forward	2
63.141.242.195	United States	147.237.77.74	law.idf.il	block-sp-trafl	forward	1
69.30.227.221	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-trafl	forward	1
63.141.231.195	United States	147.237.77.234	halag.idf.il	block-sp-trafl	forward	1
142.54.174.84	United States	147.237.77.235	sviva.idf.il	block-sp-trafl	forward	1
63.141.231.197	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-trafl	forward	1
208.110.84.67	United States	147.237.76.200	eitan.aka.idf.il	block-sp-trafl	forward	1
69.30.193.252	United States	147.237.72.166	aka.idf.il	block-sp-trafl	forward	1
31.204.128.22	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1
63.141.231.213	United States	147.237.77.176	matpash.idf.il	block-sp-trafl	forward	1
69.30.226.222	United States	147.237.72.156	aman.idf.il	block-sp-trafl	forward	1
63.141.231.195	United States	147.237.77.233	atal.idf.il	block-sp-trafl	forward	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.116.197	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
46.4.116.197	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
220.82.87.133	147.237.8.50	Korea, Republic of	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
108.168.178.253	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
108.168.178.253	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
108.168.178.253	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1
107.191.55.97	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
107.191.55.97	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
209.95.50.84	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
71.15.85.176	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
31.186.136.27	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
116.110.148.141	147.237.77.234	Vietnam	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
108.168.178.253	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
108.168.178.253	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
108.168.178.253	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
107.191.55.97	147.237.77.74	United States	law.idf.il	ET SCAN Potential SSH Scan	1
107.191.55.97	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
107.191.55.97	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
199.66.64.136	147.237.77.74	United States	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
41.220.193.155	147.237.0.19	Mozambique	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
163.172.169.150	147.237.0.16	United Kingdom	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
113.103.178.131	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.102.242.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.253.242.74	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.19.85.74	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.86.179	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
95.168.135.169	Germany	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.86.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.246.174	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
2.53.174.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.53.174.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.53.174.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.174.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
27.0.53.193	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
2.53.174.202	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
27.0.53.193	India	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.53.174.202	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
80.246.133.213	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.110.108.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
77.139.245.26	France	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.102	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.207	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.53.20.79	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.55.56.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.238.172.226	Turkey	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.53.5.127	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.176	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.226.161.161	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.28.155.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
100.92.192.120		147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	2
185.27.106.19	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
176.13.232.205	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
213.238.172.226	Turkey	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
89.139.24.22	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
79.183.58.55	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.108.140.41	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.142.9.242	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
2.55.143.212	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.236	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.26	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
77.138.230.127	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.168.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	159
80.246.138.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.85.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	4
209.88.196.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 209.88.196.250	Block	3
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.163.107	France	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.117.30.165	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
212.29.224.163	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$cpMain\$cpMain\$ct141 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
85.115.52.202	United Kingdom	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3468.gif	Block	1
46.19.86.12	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.255	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
66.102.9.6	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
109.67.5.57	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2331.jpg	Block	1
46.19.86.153	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
207.46.13.171	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/pdf/files/x'x™xæx™x•x x•xª	Block	1
84.94.37.164	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.94.37.164	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
141.226.217.240	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
77.138.67.228	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
84.94.37.164	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
144.76.120.23	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
77.139.163.107	France	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method	Block	1
46.19.86.176	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
209.88.196.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	1
84.111.109.28	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9682-he/refuah.aspx	Block	1
157.55.39.255	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1