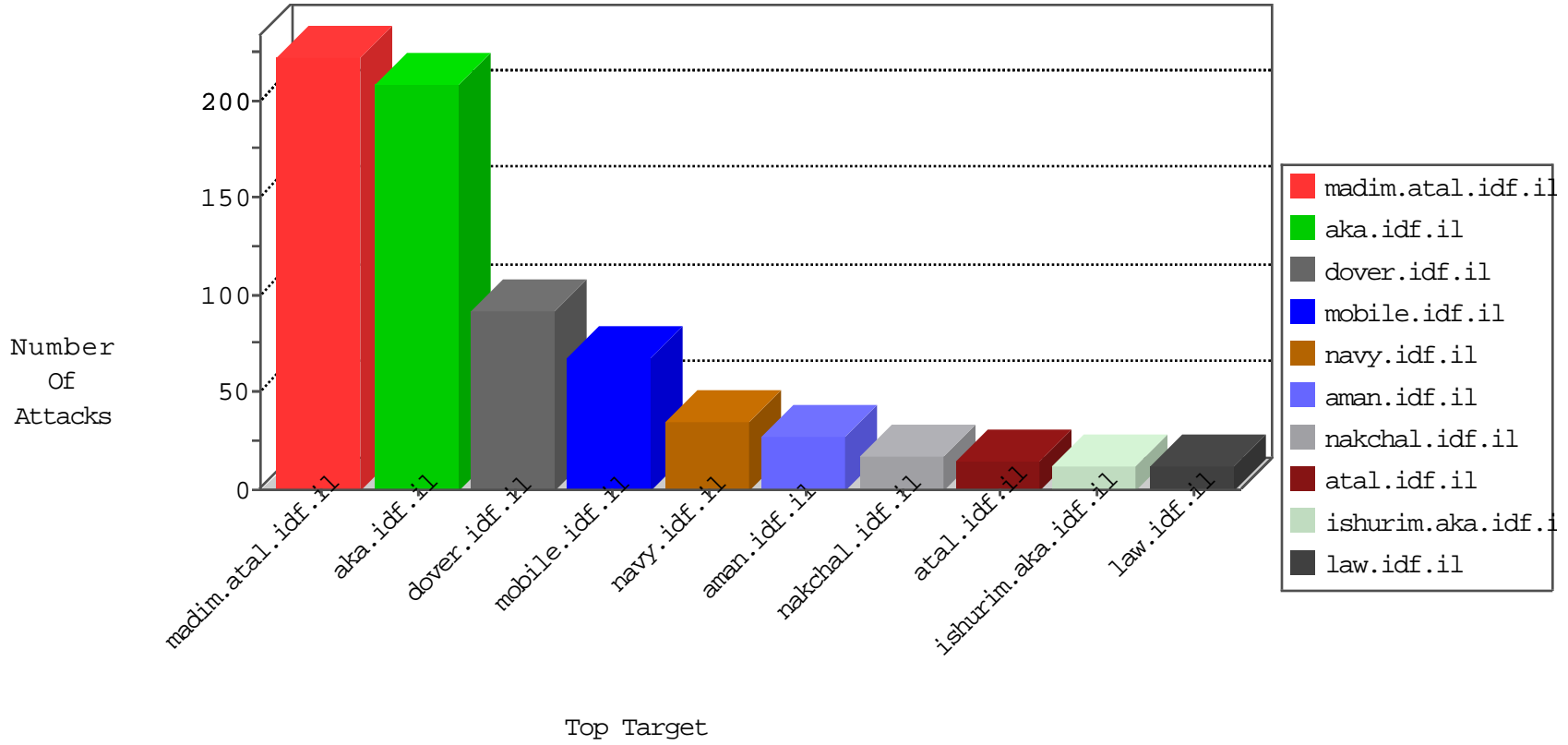


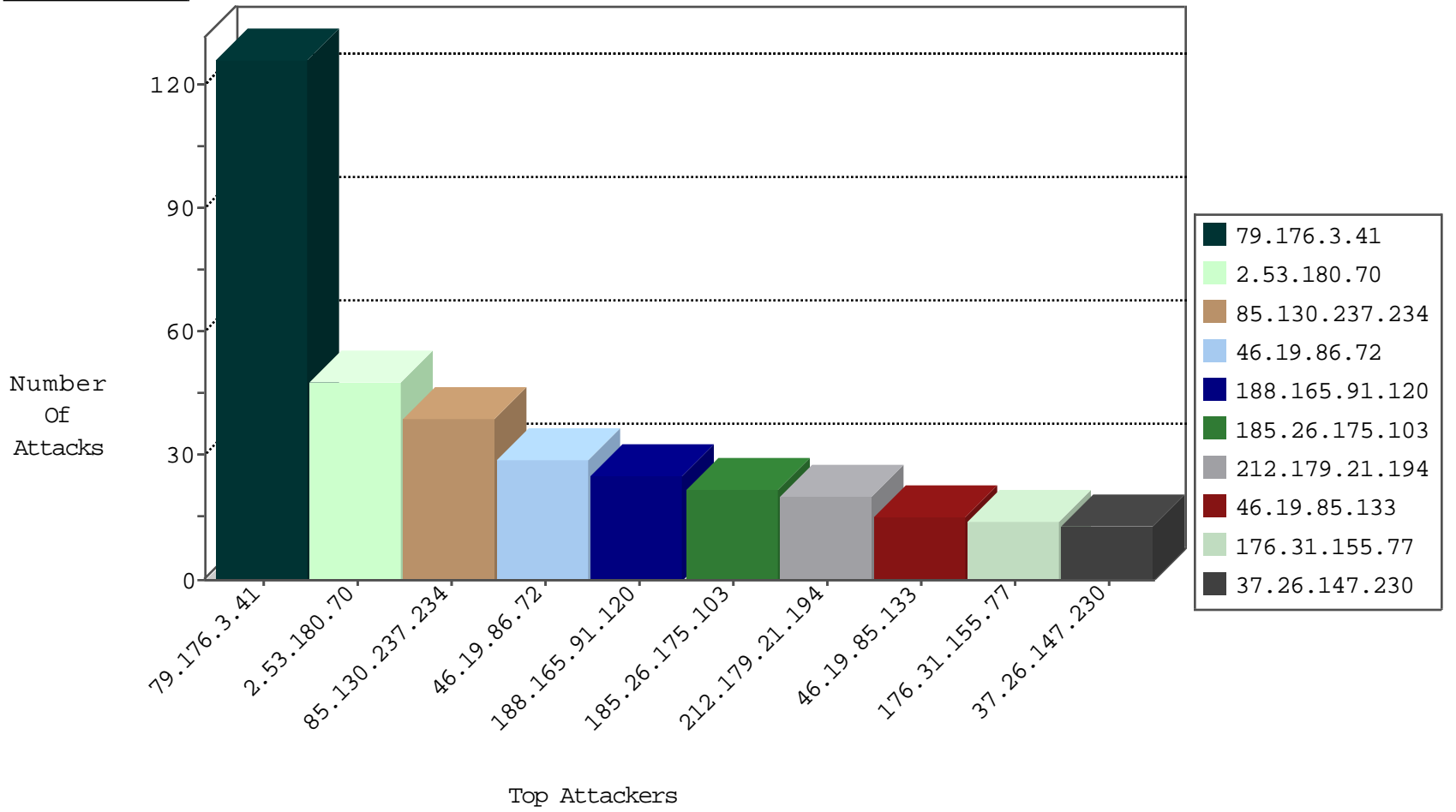
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.103.153	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
79.183.30.220	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
115.230.125.146	China	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
163.172.216.36	United Kingdom	147.237.76.44	e.refuah.idf.il	Black List	drop	1
154.16.199.217	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1
163.172.216.36	United Kingdom	147.237.76.197	e.himush.idf.il	Black List	drop	1
154.16.199.217	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
163.172.216.36	United Kingdom	147.237.76.198	e.yochalan.idf.il	Black List	drop	1
106.2.201.252	China	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
154.16.199.217	United States	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
108.59.8.70	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
108.59.8.70	United States	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
46.19.85.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.3.147.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
23.82.46.210	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
107.178.208.177	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.50.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.84.108	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.69.240	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.227.67.172	147.237.72.167	Sweden	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.117.244.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.225.149	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.146.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.247.16	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
23.82.46.210	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.119.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.60.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.104.213	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.127.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.252	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
46.227.67.172	147.237.72.166	Sweden	aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.24.164	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.70.211.10	147.237.77.216	Europe	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.130.237.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
85.130.237.234	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	14
46.19.85.133	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	13
85.130.237.234	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
176.13.249.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
212.179.21.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	10
192.117.162.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
212.179.21.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
192.101.80.14	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.250.241	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
185.3.147.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.8.204.8	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
37.26.148.237	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.145.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.157	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.3.147.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.27.211	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.157	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.55.12.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.148.232	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
84.109.39.0	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.12.244	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.53.27.211	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.32.200.232	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.157.117.73	Iceland	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.55.14.33	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.186.28	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.139.151.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
157.157.117.73	Iceland	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
79.178.169.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.32.179.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.248.208	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.141	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.32	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
2.53.186.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.120.126.75	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.253.128.223	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
213.8.204.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
185.3.147.167	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.53.186.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
46.19.86.188	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
104.198.219.118	United States	147.237.76.42	refuah.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
185.26.175.103		147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.79	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
80.246.133.47	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	alert	2
109.253.138.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.54.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
5.144.63.90	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
109.253.192.171	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.3.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
2.53.180.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
46.19.86.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
37.26.147.230	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	13
87.71.29.74	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	6
80.246.130.246	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
2.53.159.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.80.248.1	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.86.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.11.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.102.174	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	2
185.3.147.191	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
31.19.128.202	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/rabanut/general.aspx	Block	2
46.19.86.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.202.13	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter utm_medium in www.aka.idf.il/ishurim/main	None	1
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method zh55thgkjqz in URL	Block	1
207.46.13.64	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1
2.53.186.28	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.71.26.143	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
66.249.64.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9841-he/refuah.aspx	Block	1
27.152.244.33	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
79.181.51.162	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general	Block	1
77.127.77.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.64	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
5.28.145.246	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.240	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
2.53.173.109	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
80.246.130.87	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.138.75.144	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
5.29.68.63	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
79.179.96.1	Israel	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	1
192.187.101.170	United States	147.237.76.86	navy.idf.il	Admin Blocking	Block	1
77.139.18.220	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
46.19.86.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
136.243.67.234	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
5.29.78.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyu	Block	1
79.179.96.1	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/wp-login.php	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mail/kapats	Block	1
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
2.53.186.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.81.95.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/guyus	Block	1
77.139.75.52	France	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$txtSearch in www.aka.idf.il/main/giyus/forms.aspx	None	1
27.152.244.33	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 27.152.244.33	Block	1
79.181.51.162	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	1