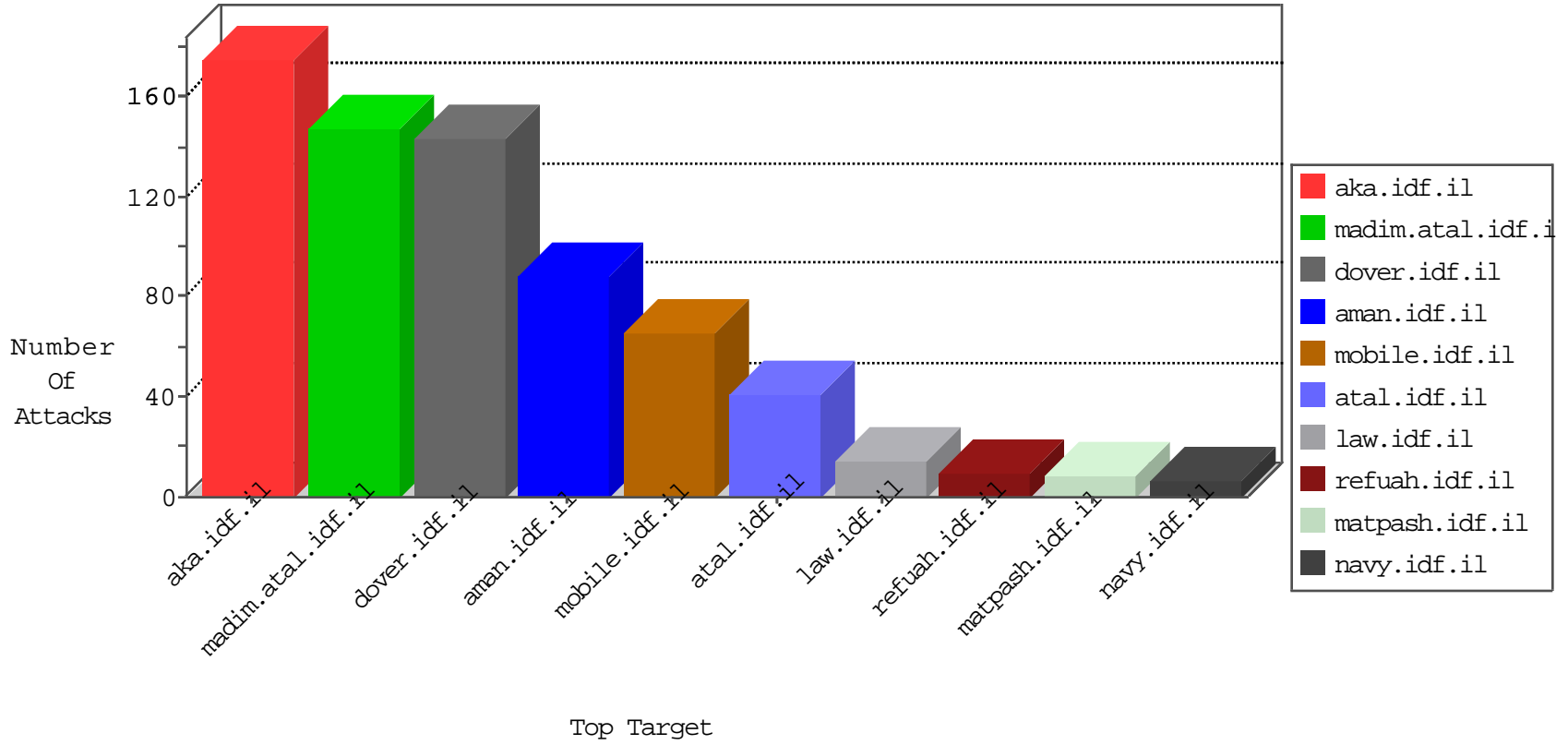


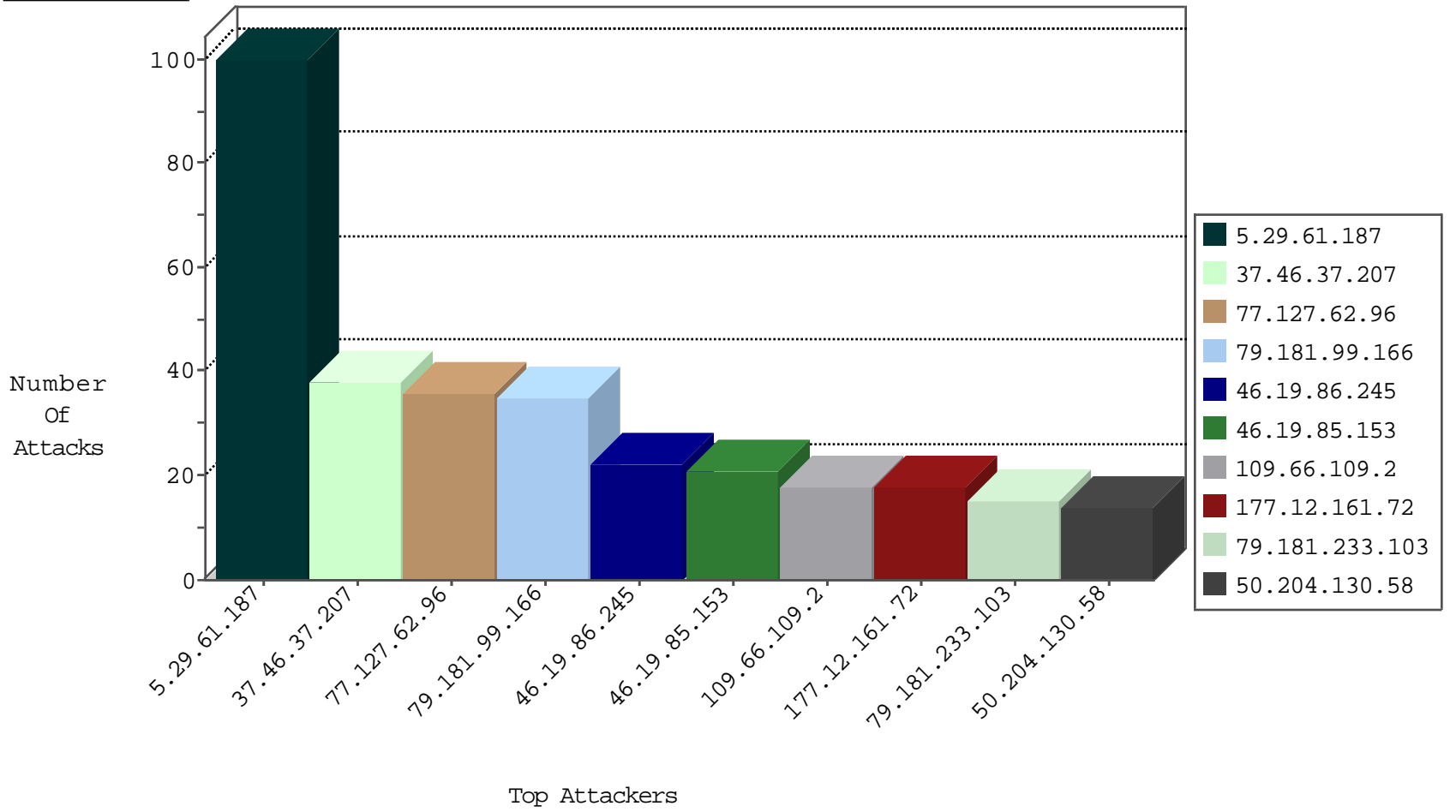
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.233.103	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
78.129.161.50	United Kingdom	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.201.216.68	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.27.116	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	6
177.12.161.72	Brazil	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
83.149.126.98	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
83.149.126.98	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
177.12.161.72	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	14
184.168.27.116	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
173.201.216.68	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	3
62.210.97.79	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
40.121.139.43	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
203.106.184.157	147.237.77.216	Malaysia	dover.idf.il	ET SCAN NMAP -sS window 4096	1
113.86.186.198	147.237.77.216	China	dover.idf.il	portscan: TCP Distributed Portscan	1
104.207.141.110	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.130.239	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
208.80.155.255	147.237.77.216	United States	dover.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	1
203.106.184.157	147.237.77.216	Malaysia	dover.idf.il	ET SCAN NMAP -sS window 1024	1
117.43.238.111	147.237.72.14	China	dover.idf.il(olc	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.207.141.110	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -sS window 2048	1
104.207.141.110	147.237.76.201	United States	e.atal.idf.il	ET SCAN NMAP -f -sS	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.127.62.96	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
109.66.109.2	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
50.204.130.58	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
93.172.144.196	Israel	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.128.48.130	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
109.67.148.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
37.46.37.207	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	10
79.181.99.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
79.181.233.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.46.37.207	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		monitor	8
80.249.198.65	Russian Federation	147.237.77.216	dover.idf.il	drop		drop	8
46.243.150.195	Bahrain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
79.177.244.98	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
153.31.113.21	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.37.207	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
31.154.81.0	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
37.46.37.207	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
185.3.147.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.181.99.166	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
37.46.37.207	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.181.106.58	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
37.142.95.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	5
79.182.43.61	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
109.253.207.41	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
185.120.124.46	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
75.104.64.128	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.133.209.236	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.143.38.222	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.87	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.38.222	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
100.92.237.230		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
5.29.227.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.116.39.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	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
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.177.202.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
89.138.172.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.37.207	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
197.17.35.158	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
220.247.247.74	Sri Lanka	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
5.22.134.82	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.105.115.179	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.3.125	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
185.3.147.61	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.61.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
46.19.86.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
89.138.172.4	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	6
40.77.167.60	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	3
176.13.249.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.142.91	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	3
84.108.42.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.243.55.136	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	2
5.29.239.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
79.177.134.115	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.177.134.115	Block	2
23.88.118.27	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
109.253.209.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
95.86.80.150	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
5.29.227.31	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.177.134.115	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
66.102.6.3	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	1
37.142.233.114	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
141.226.161.24	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
89.138.172.4	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.53.5.12	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.79.165	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/m/	Block	1
46.117.130.98	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.67.158.238	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/giyus.asp	Block	1
2.53.136.248	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/text.css	Block	1
77.125.86.187	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/popups/markivsachar.aspx	None	1
192.243.55.138	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	1
46.120.74.41	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
5.102.195.240	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
79.179.102.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8857-he/refuah.aspx	Block	1
46.19.86.34	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
178.94.126.27	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
89.139.183.35	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/sachar/newsarchive.aspx	Block	1
2.53.136.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
77.138.80.38	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
192.243.55.138	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp?moduleid=3&catid=22704	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/giyus	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8859-he/refuah.aspx	Block	1
185.120.124.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.172.144.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
77.138.228.131	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
213.57.15.248	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
46.121.117.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.154.81.20	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/giyus/general.aspx	Block	1
125.77.28.26	China	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
84.229.50.87	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
192.243.55.135	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58568&docid=65100	Block	1
46.116.31.7	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1