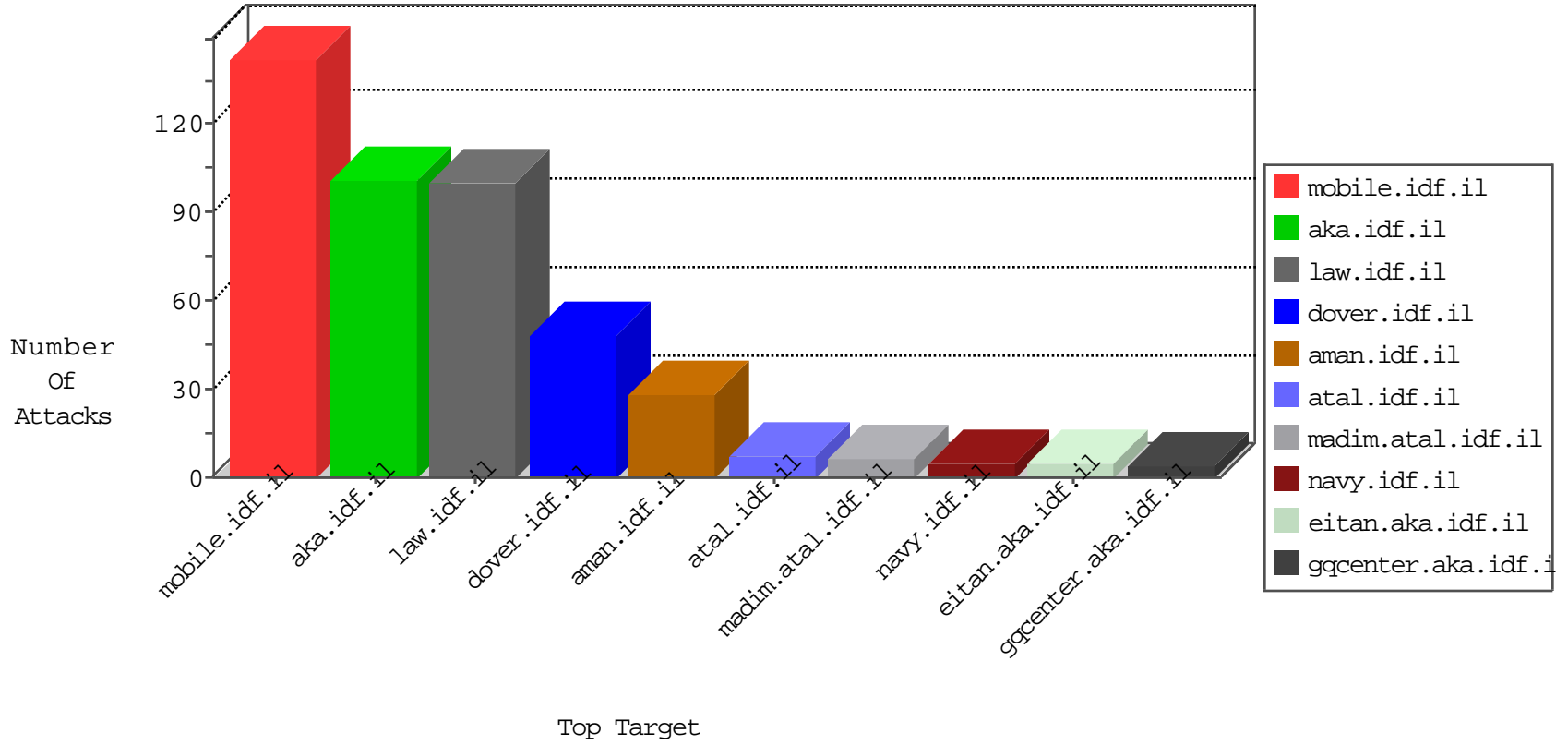


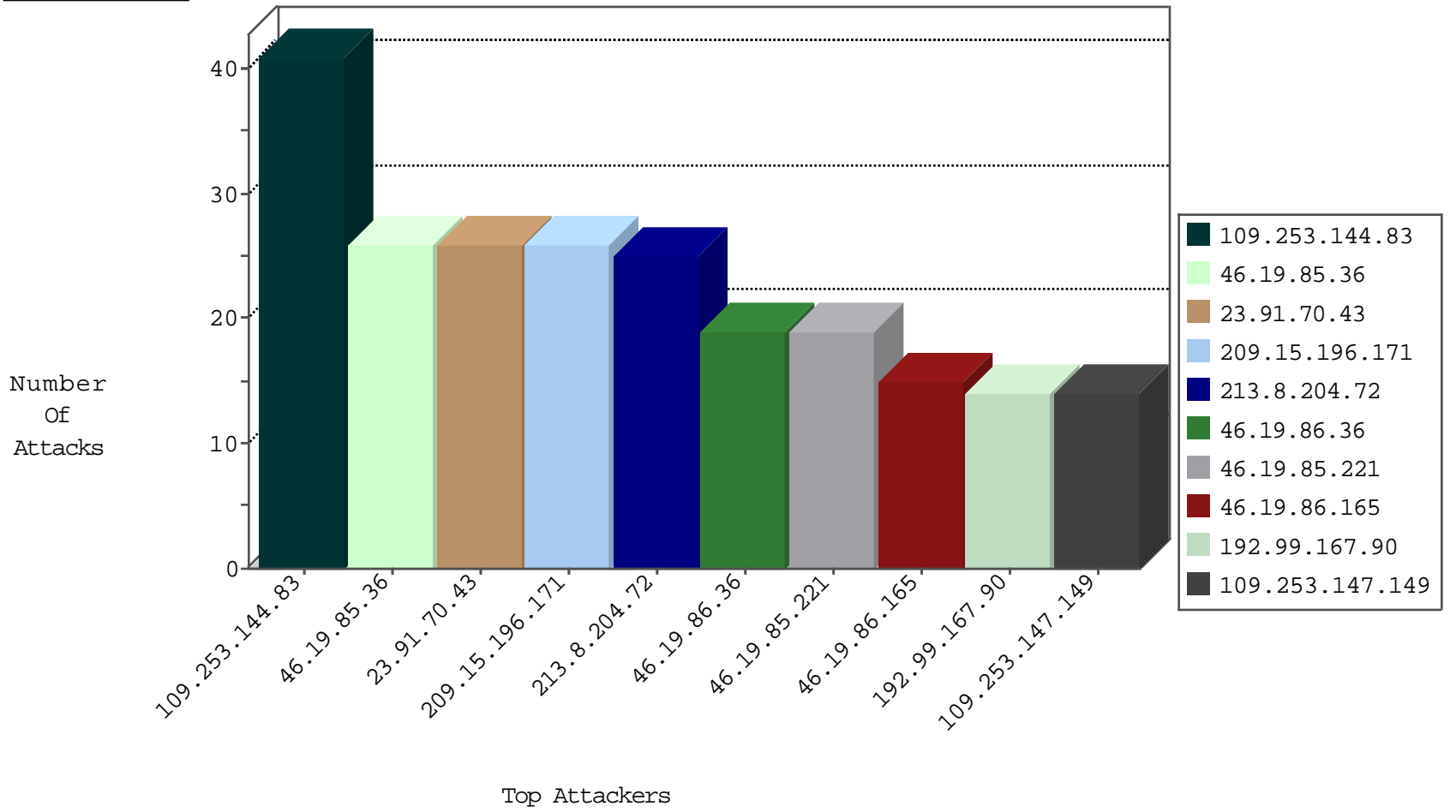
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.44.110.25	United States	147.237.76.197	e.himush.idf.il	Black List	drop	1
93.158.215.26	Netherlands	147.237.76.148	ggcenter.aka.idf.il	Black List	drop	1
198.44.110.15	United States	147.237.76.148	ggcenter.aka.idf.il	Black List	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
209.15.196.171	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
184.168.46.74	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
192.99.167.90	Canada	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.43	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
64.34.186.9	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.43	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
209.15.196.171	Canada	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	5
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
52.1.90.117	United States	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
52.1.90.117	United States	147.237.77.243	mobile.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
209.15.196.171	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	14
23.91.70.43	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
184.168.46.74	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
64.34.186.9	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
192.99.167.90	147.237.77.74	Canada	law.idf.il	SQL Injection - Select From	8
50.77.136.81	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	6
158.85.253.245	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	2
108.168.178.253	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
89.216.119.94	147.237.76.176		test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
66.249.66.131	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
46.172.91.21	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
46.161.40.17	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
40.121.139.43	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
108.168.178.253	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
108.168.178.253	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
89.216.119.94	147.237.76.176		test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
85.214.64.13	147.237.77.212	Germany	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.91.21	147.237.77.233	Ukraine	atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.91.21	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
46.97.58.78	147.237.72.217	Romania	e.idf.il	ET SCAN NMAP -sS window 1024	1
108.168.178.253	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.253.144.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
213.8.204.72	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
46.19.85.221	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.86.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
109.253.147.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.146.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.21.169	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.165	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.86.165	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.120.53.251	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.142.100	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.210.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.166.244.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.204.72	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
217.55.244.22	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
87.68.42.152	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
46.19.85.36	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.36	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
68.131.64.241	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
213.8.204.72	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.36	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.36	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
5.102.253.201	Israel	147.237.77.243	mobile.idf.il	SYN Attack		monitor	2
37.26.149.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
67.58.15.97	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
176.13.17.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
5.29.249.15	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
68.142.232.17	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
89.138.176.116	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
185.32.179.58	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.17.155	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
141.212.122.86	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
52.198.122.46	Japan	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
188.120.148.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.53.175.44	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.13.17.155	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.80	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.65.171.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
5.102.253.201	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.144.83	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
46.19.85.221	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.253.147.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.162	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
82.166.244.220	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
75.127.60.26	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 75.127.60.26	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	2
46.19.86.159	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.147.149	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.210.93	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.20	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
12.11.109.225	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
66.249.66.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/assetlinks.json	Block	1
157.55.39.155	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/60984.pdf	Block	1
46.19.86.55	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
31.154.81.4	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
176.13.17.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.149.191	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.76.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/70124.doc	Block	1
31.154.81.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
75.127.60.26	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
66.249.66.183	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
207.46.13.106	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/ylcebowm67a	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
109.64.4.91	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/ult.aspx	Block	1
2.53.60.115	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
68.131.64.241	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for eitan.aka.idf.il/1094-8149-en/eitan.aspx	None	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx	Block	1
31.154.81.4	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
79.177.172.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachr/	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8859-he/refuah.aspx	Block	1
217.69.133.225	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter fb709480 in aka.idf.il/giyus/	None	1
2.53.173.24	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
109.253.142.100	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.238	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
66.249.64.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/67706.pdf	Block	1
31.154.81.4	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
157.55.39.104	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.77	Block	1