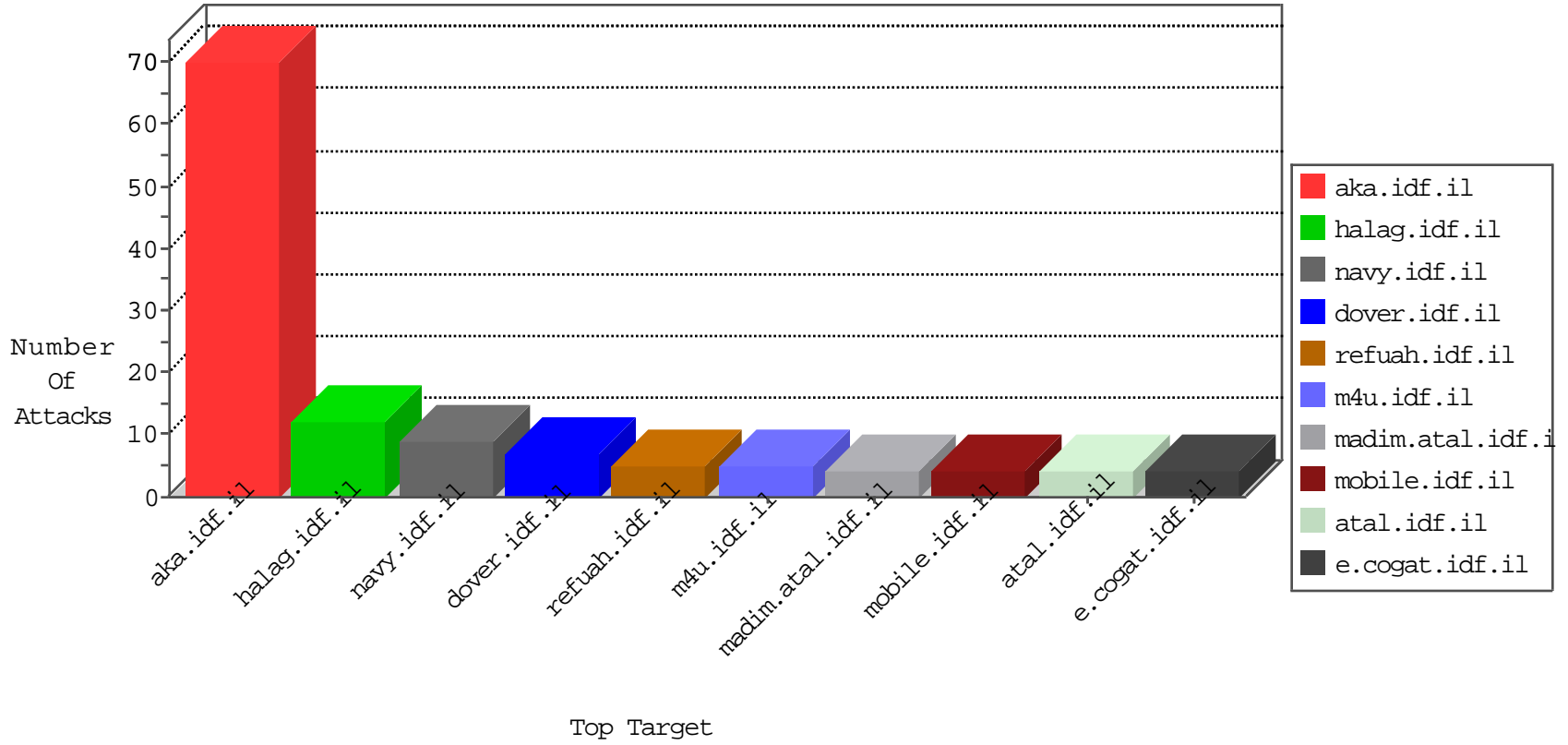


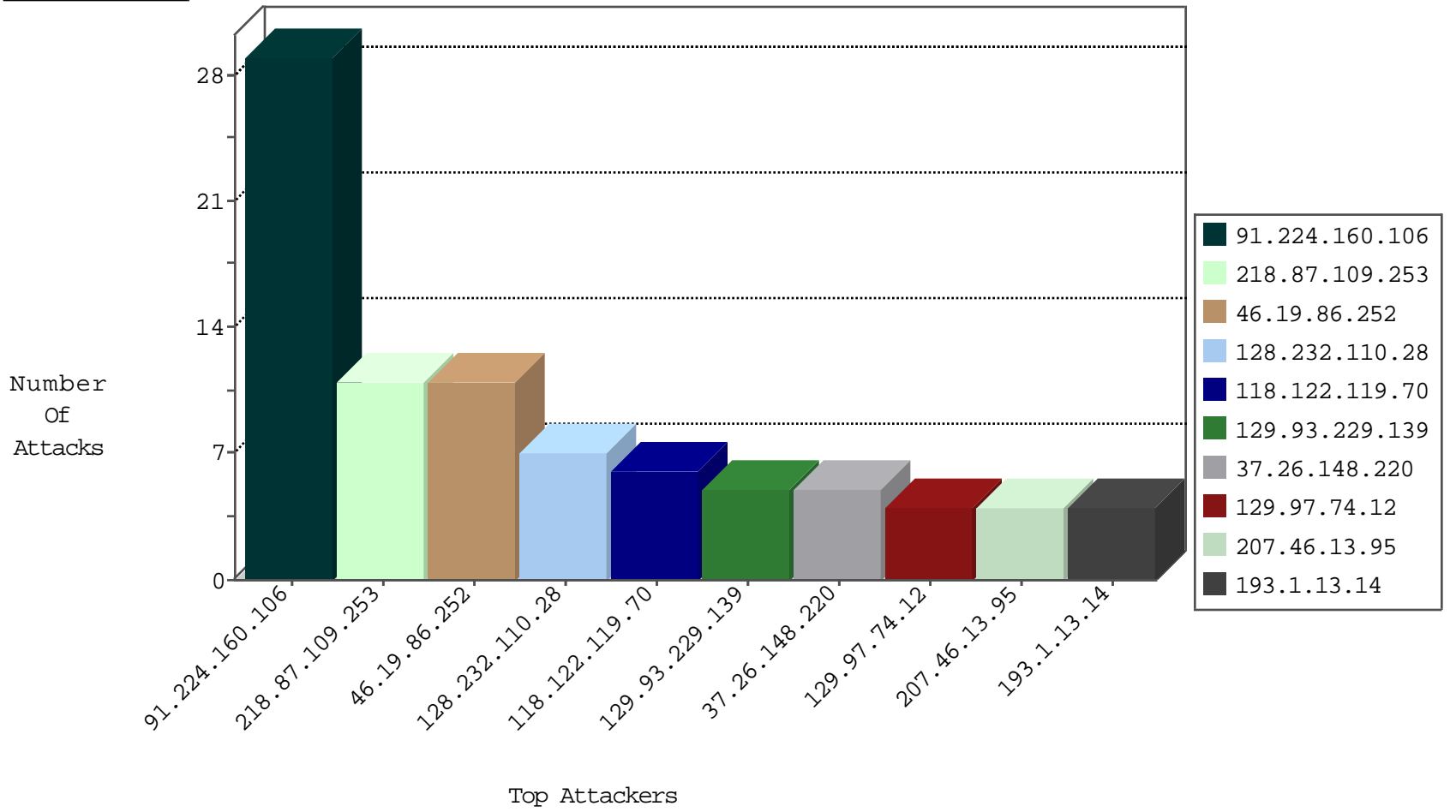
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.13	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
118.122.119.70	China	147.237.76.38	e.e.meitav.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
165.242.90.128	Japan	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
91.224.160.106	Netherlands	147.237.77.205	prisha.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
195.113.161.82	Czech Republic	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
118.122.119.70	China	147.237.76.34	yohalan.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.207.27	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.224.160.106	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.148	Netherlands	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
66.212.179.106	147.237.0.35	Canada	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
40.121.139.43	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
192.81.216.190	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
40.121.139.43	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
103.244.59.205	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
93.158.203.149	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
41.180.8.100	147.237.77.121	South Africa	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
40.121.139.43	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
101.178.206.92	147.237.77.226	Australia	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.252	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.252	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.148.220	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.3.147.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
207.46.13.95	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.237.146.28	Czech Republic	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.143.217.19	Iran, Islamic Republic of	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
62.201.219.91	Iraq	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
128.232.110.28	United Kingdom	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
66.212.179.106	Canada	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
141.212.122.111	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
128.232.110.28	United Kingdom	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
116.193.152.154	China	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
141.212.122.107	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
128.232.110.28	United Kingdom	147.237.0.35	akaws.idf.il	drop		drop	1
101.199.112.45	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
157.55.39.99	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
128.232.110.28	United Kingdom	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
118.122.119.70	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
77.237.146.28	Czech Republic	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
141.212.122.109	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
128.232.110.28	United Kingdom	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
141.212.122.85	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
118.122.119.70	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
93.174.95.106	Netherlands	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
1.39.24.228	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.110	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
128.232.110.28	United Kingdom	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.253.230.226	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
192.81.216.190	United States	147.237.0.200	m4u.idf.il	drop		drop	1
141.212.122.86	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
118.122.119.70	China	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
101.178.206.92	Australia	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.110	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
116.193.152.154	China	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.106	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
118.122.119.70	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
101.178.206.92	Australia	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2801.jpg	Block	1
104.128.144.131	Canada	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/redirect.php	Block	1
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2802.jpg	Block	1
157.55.39.29	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/general.aspx	Block	1
68.180.228.238	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
207.46.13.95	United States	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
68.180.229.90	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1073-he/nakhal.aspx	Block	1
207.46.13.166	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
77.237.146.28	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1