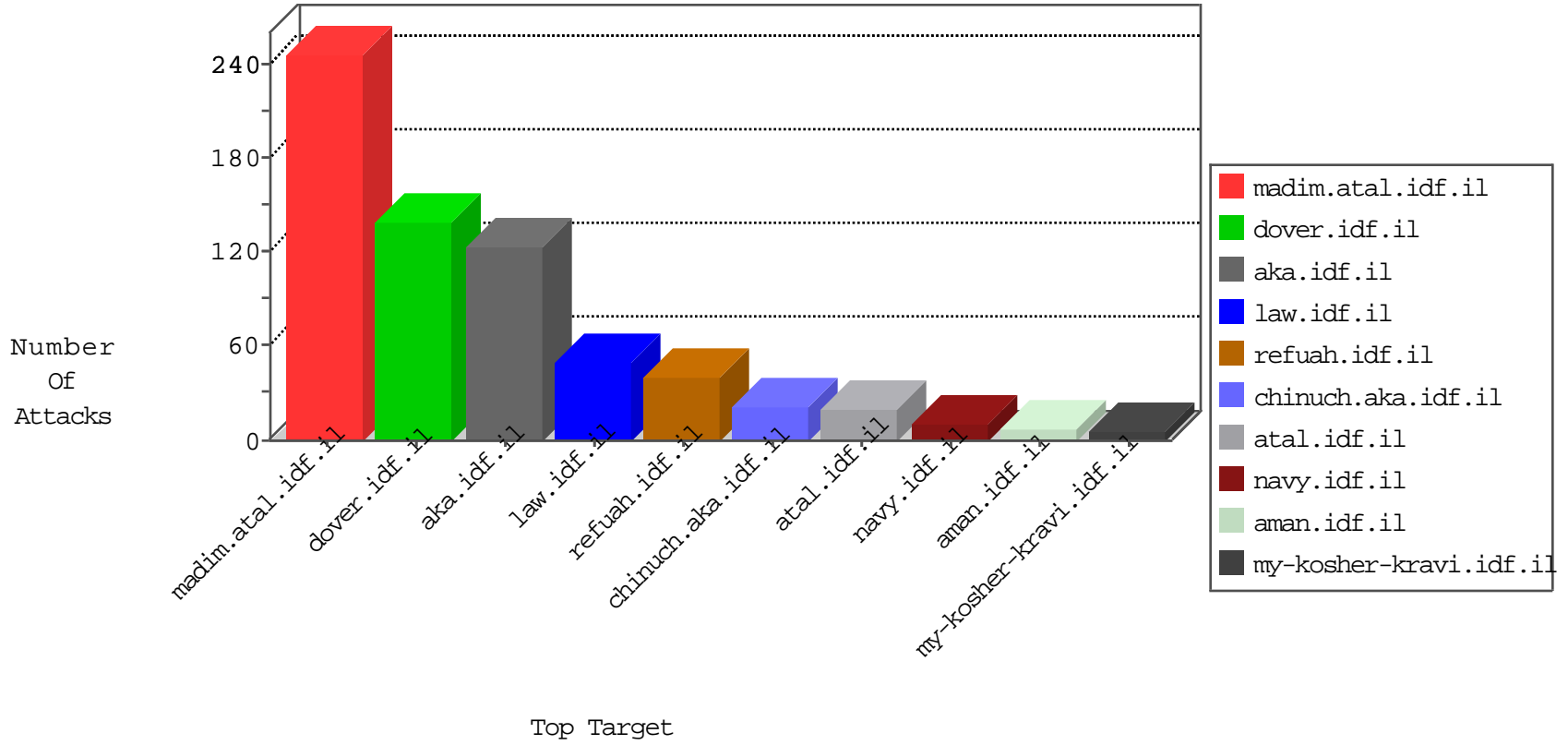


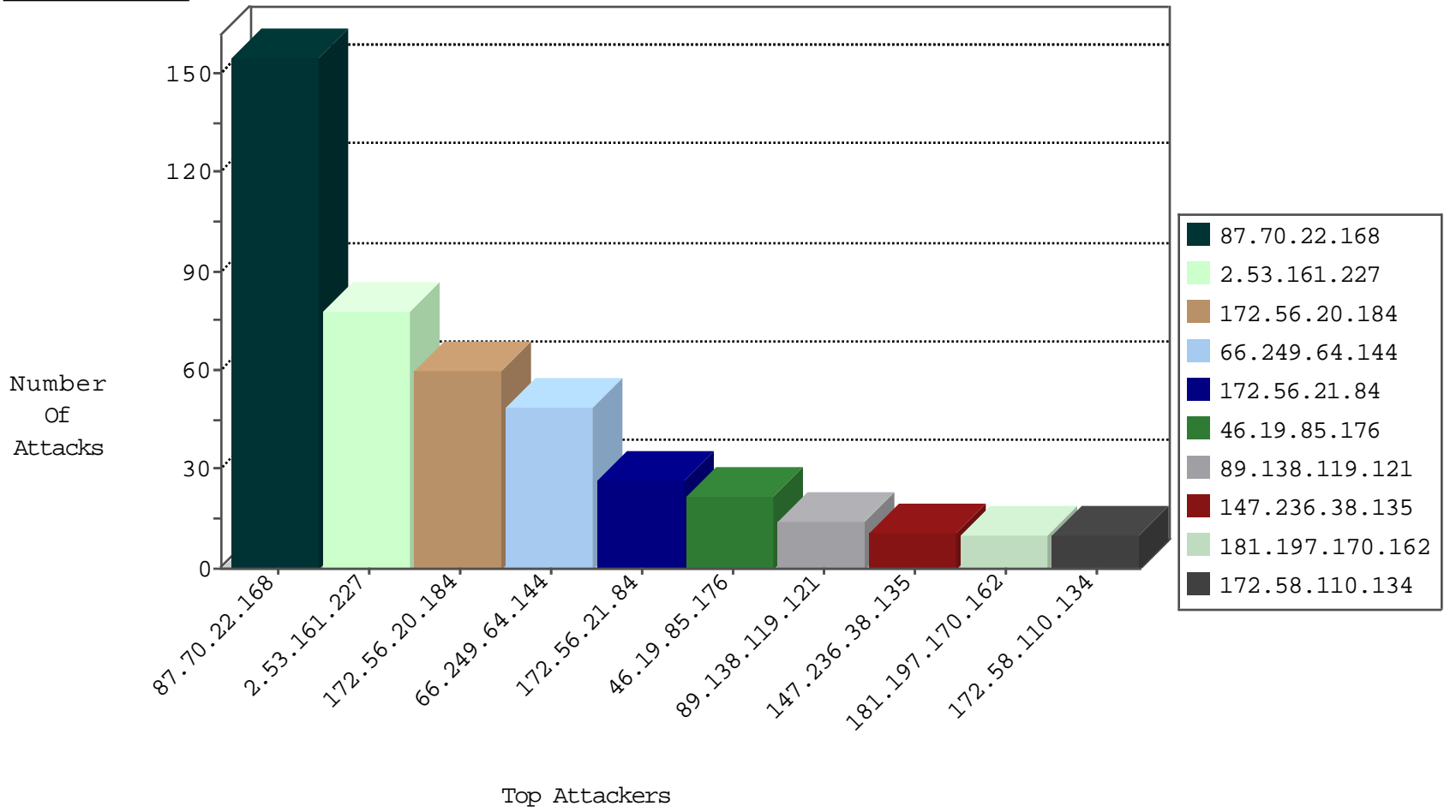
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
198.82.160.238	United States	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
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.93.229.138	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	2
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.93.229.139	United States	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	1
200.19.159.34	Brazil	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
80.82.70.24	Netherlands	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.99	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
192.33.90.67	Switzerland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
85.64.146.68	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
198.133.224.147	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
120.132.50.135	China	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	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
51.254.143.238	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
66.240.236.119	United States	147.237.0.16	my-kosher-kravi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.144	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	49
62.90.131.234	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	6
84.93.84.77	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
50.84.213.146	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
189.161.173.106	147.237.8.46	Mexico	e.chimuch.idf.il	ET SCAN NMAP -sS window 1024	1
188.0.236.165	147.237.0.16	Moldova, Republic of	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
161.18.148.114	147.237.77.234	Colombia	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.64.180.208	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.179.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
188.0.236.165	147.237.0.35	Moldova, Republic of	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN NMAP -sS window 1024	1
116.7.243.198	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
172.56.21.84	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
172.56.20.184	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
172.56.20.184	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
89.138.119.121	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
172.56.21.84	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
147.236.38.135	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	11
172.56.20.184	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
172.56.20.184	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
77.139.153.53	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
81.218.101.66	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.176	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.137.106	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.176	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.63	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
176.13.232.162	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
172.56.20.184	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
172.56.20.184	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
87.69.36.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.86.202	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.146.143	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	3
192.169.7.223	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
176.13.249.99	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
172.58.110.134	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
88.202.218.230	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	3
37.26.146.143	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
172.58.110.134	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
88.202.218.230	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
87.69.79.16	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
87.69.79.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
70.26.167.199	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
80.82.70.24	Netherlands	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
46.19.85.250	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.57	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
84.229.4.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.64.169.81	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.13	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
80.246.140.221	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
2.53.138.162	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.26	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
172.58.110.134	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
157.55.39.19	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
193.28.155.101	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
176.13.240.202	Israel	147.237.72.166	aka.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
87.70.22.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	155
2.53.161.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
181.197.170.162	Panama	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 181.197.170.162	Block	9
185.32.179.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.195.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.82.70.24	Netherlands	147.237.77.216	dover.idf.il	Multiple NULL Character in Method from 80.82.70.24	Block	3
37.26.146.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.82.70.24	Netherlands	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 80.82.70.24	Block	2
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 93.158.152.52	Block	2
109.253.136.108	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	2
200.111.107.58	Chile	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/index.php	Block	1
89.138.119.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	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
157.55.39.135	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
207.46.13.22	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
62.90.131.234	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
80.82.70.24	Netherlands	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
213.57.70.6	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-8103-he/dover.aspx.	Block	1
66.102.9.26	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
181.197.170.162	Panama	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
87.68.42.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
2.53.177.181	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
213.57.215.69	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
79.181.207.22	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/	Block	1