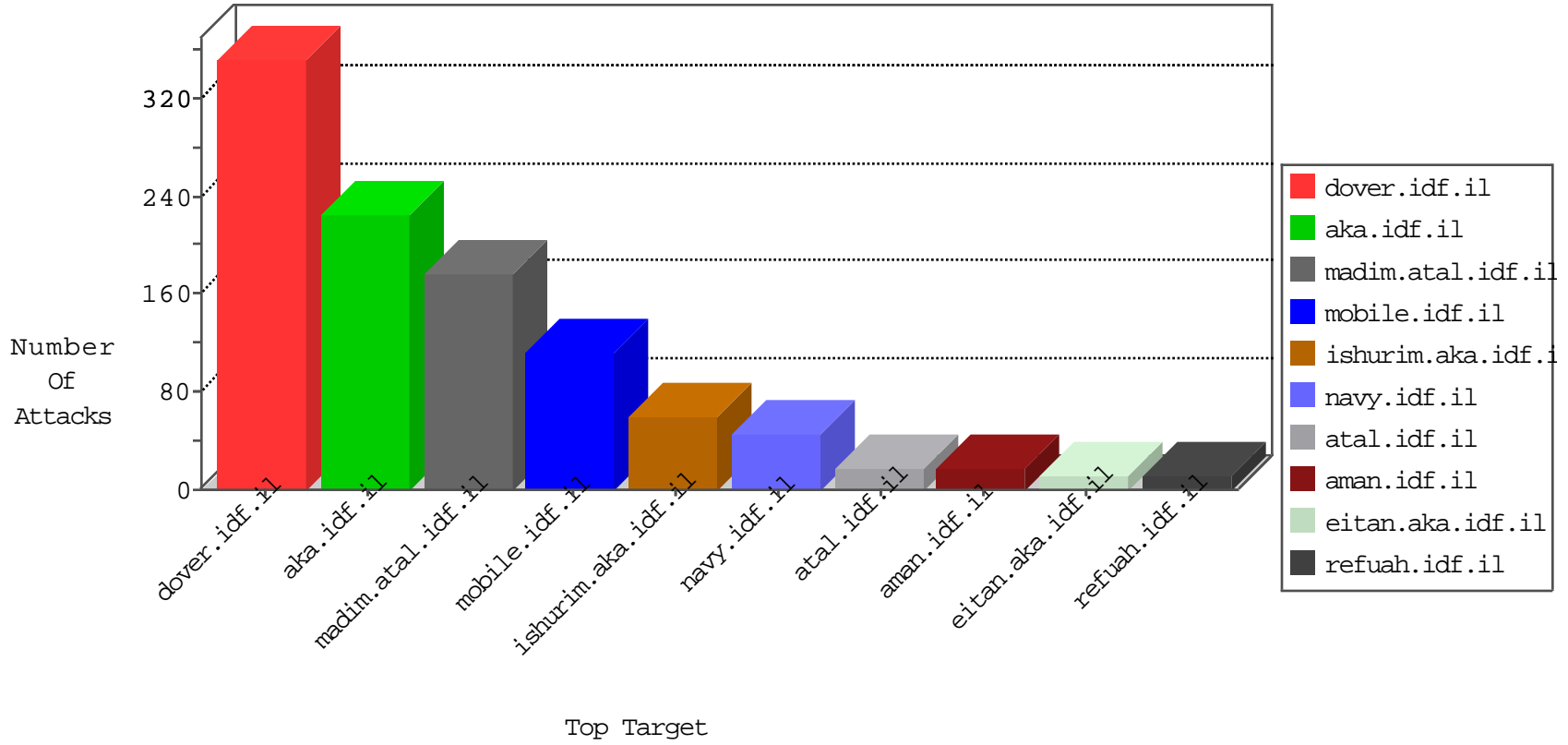


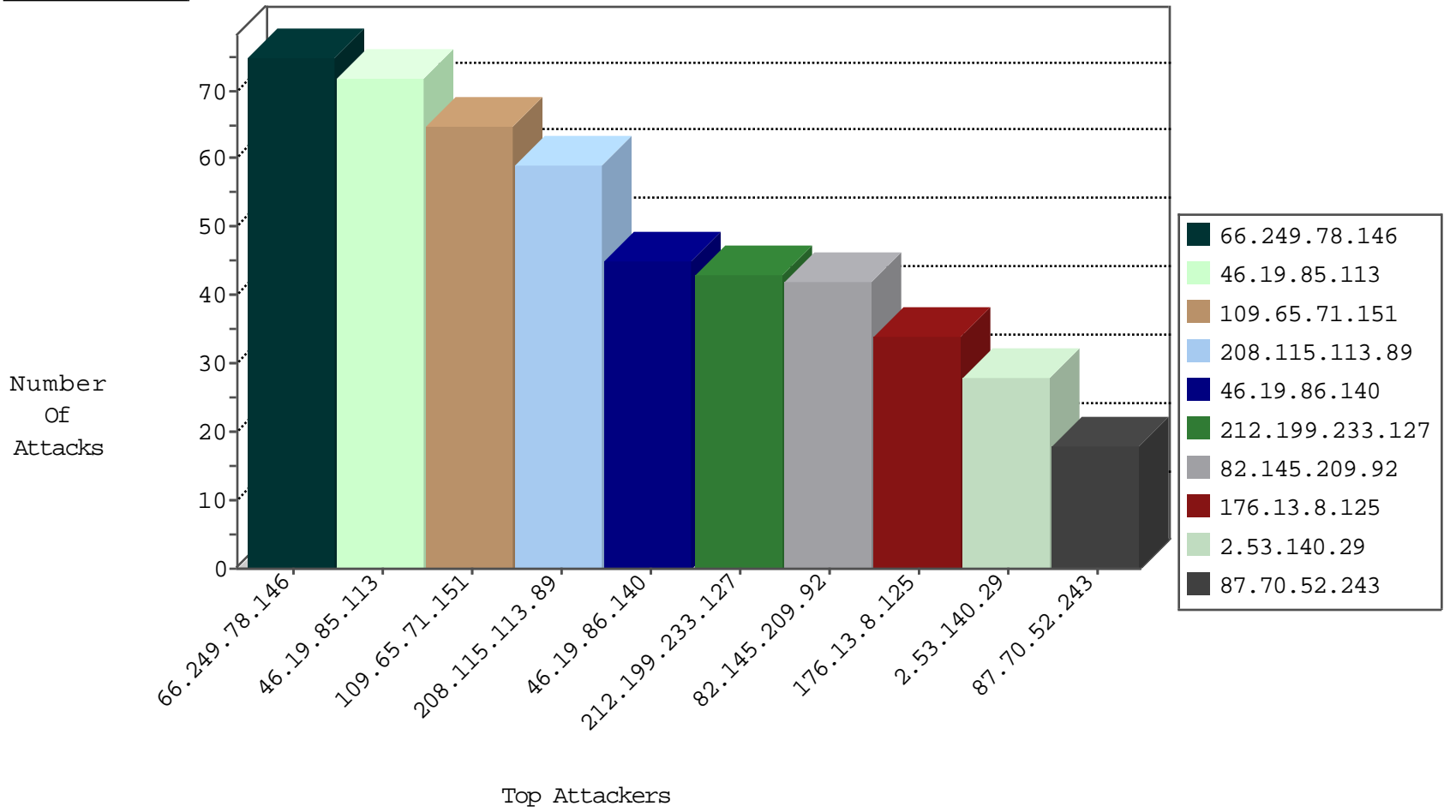
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.233.127	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	395
2.53.140.29	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
82.145.209.92	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	42
79.177.155.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
185.94.111.1	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
172.82.142.122	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
211.220.63.148	Korea, Republic of	147.237.72.167	ishurim.aka.idf.	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.176.148.232	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	16
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
211.220.63.148	147.237.72.167	Korea, Republic of	ishurim.aka.idf.il	ET WEB_SERVER Possible bash shell piped to dev tcp Inbound to WebServer	1
183.56.166.188	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
115.47.12.162	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.62.93	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
213.151.52.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
163.172.140.23	147.237.77.121	United Kingdom	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.65.199.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	75
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
176.13.8.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
2.53.140.29	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.177.185.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
162.243.99.146	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.253.135.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.113	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.205.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.219.209	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.67.204.38	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
2.53.160.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.0.46	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.26.146.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.154.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.102.254.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
157.55.39.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.0	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
50.116.28.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
141.8.132.95	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.140	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
95.35.88.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.46.39.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
103.1.70.232	Malaysia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.148.27.130	Germany	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
188.96.125.10	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.135	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.130.240.210	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.0.116.177	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.182	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.162.199.197	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
203.110.158.227	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
81.218.204.225	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
109.65.199.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.71.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
46.19.85.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
46.19.86.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
80.246.136.3	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	8
176.13.8.125	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
178.137.90.202	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	3
109.253.135.188	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.177.185.55	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	2
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.19.85.40	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 46.19.85.40 (Open Mode)	None	1
79.177.96.227	Israel	147.237.76.86	navy.idf.il	Cookie Tampering on cookie __atrf: Expected ab/	None	1
46.36.67.19	Lithuania	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
157.55.39.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/rabanut/61998	Block	1
87.70.79.184	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1589-en/dover.aspx	Block	1
188.120.148.104	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
46.36.67.19	Lithuania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
2.53.48.184	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
174.129.228.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
87.71.34.117	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	1
46.19.85.113	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
114.76.34.180	Australia	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.246.130.24	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
46.121.30.38	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.53.190.206	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
176.13.0.46	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
94.230.86.240	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
70.170.81.95	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.19.85.219	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
144.76.14.84	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1524-en/	Block	1
66.102.6.188	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
17.142.155.123	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/apple-app-site-association	Block	1
109.64.223.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
79.177.92.61	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
216.218.206.68	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
149.78.84.162	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
84.228.205.31	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1