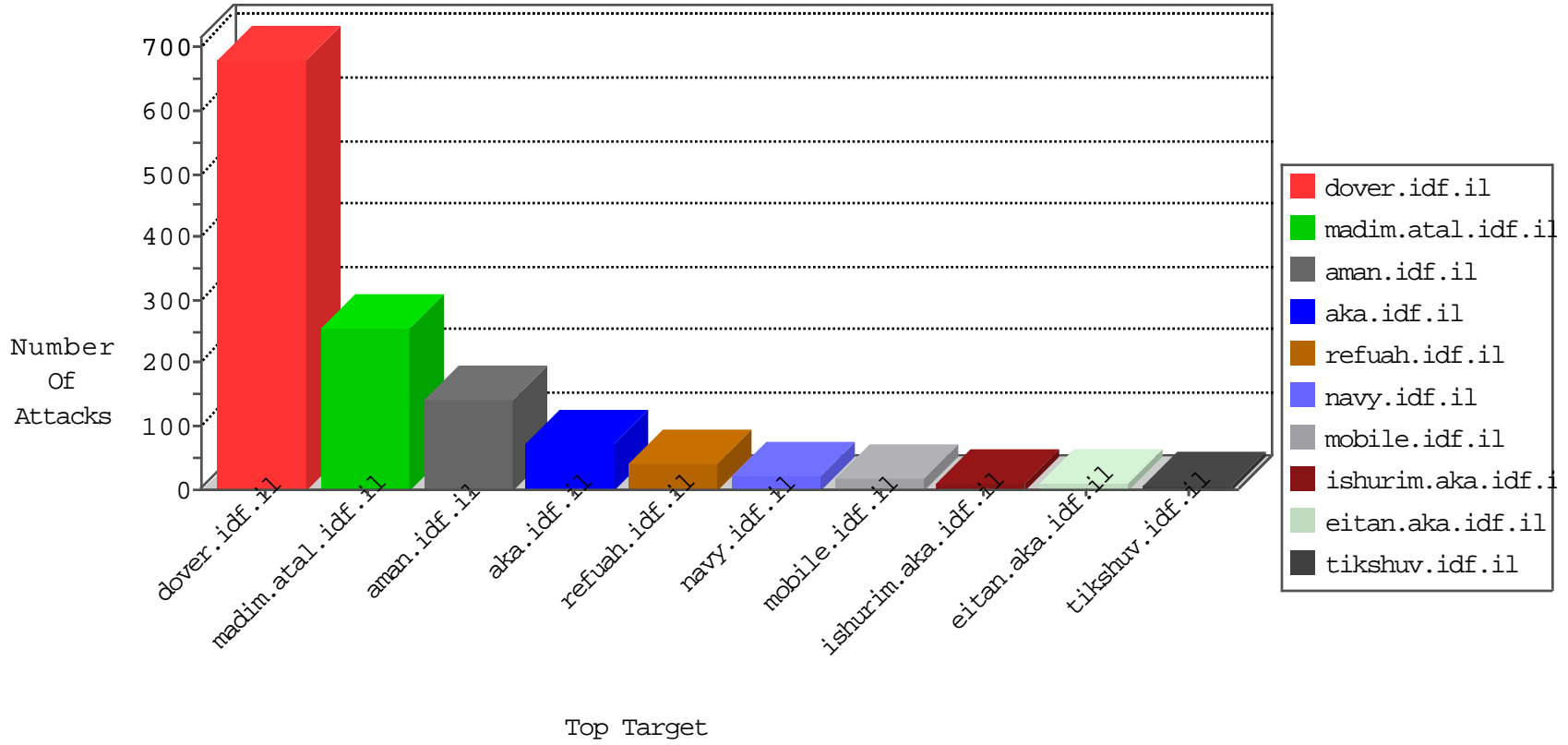


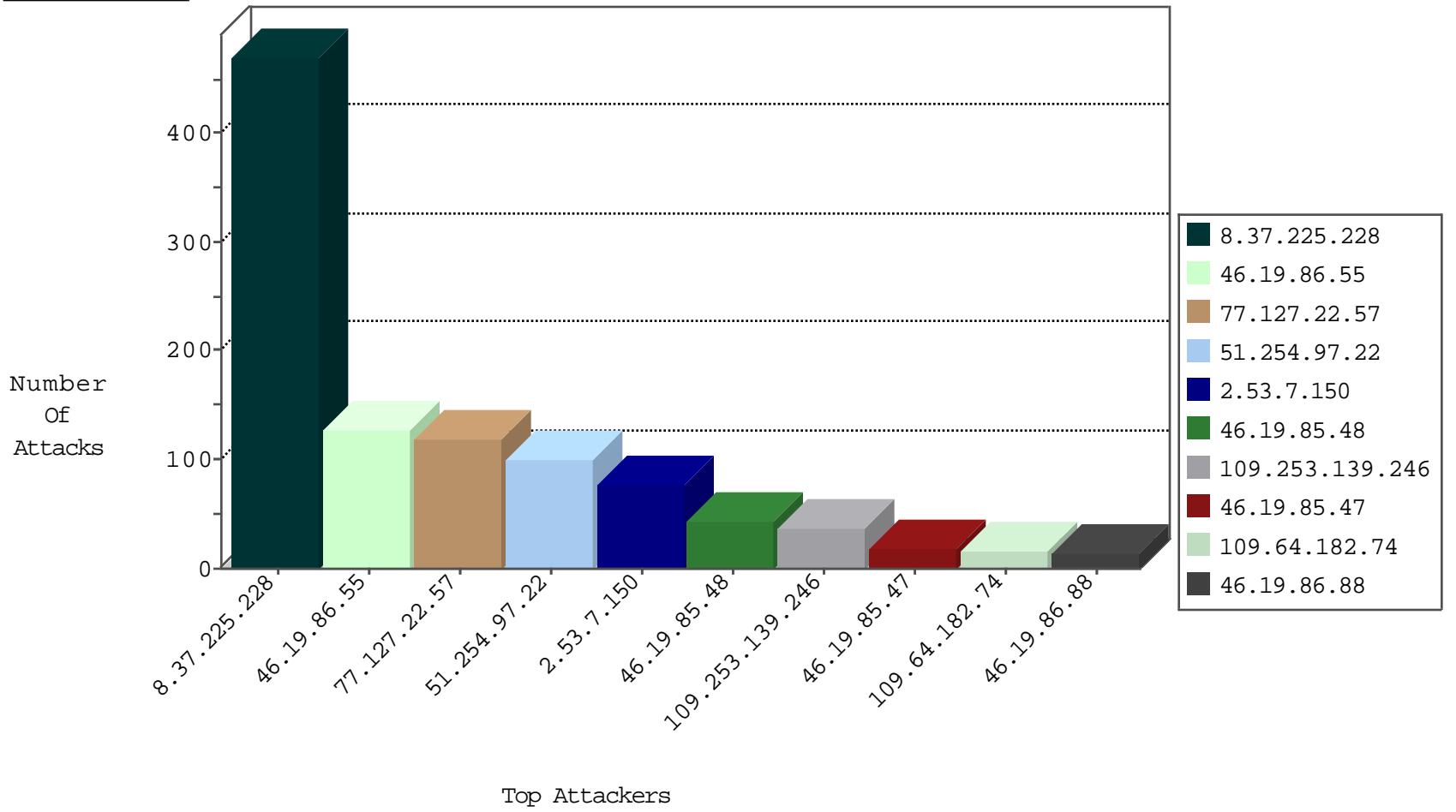
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.225.228	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	61
109.253.195.53	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	27
8.37.225.228	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	25
77.125.7.150	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
8.37.225.228	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
79.180.200.120	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
141.212.122.116	United States	147.237.76.38	e.e.meitav.idf.i	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.38	e.e.meitav.idf.i	Black List	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.97.22	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	101

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
128.232.110.28	147.237.8.14	United Kingdom	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.158	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
77.252.26.51	147.237.77.61	Poland	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
77.252.26.51	147.237.77.61	Poland	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
66.249.64.124	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
210.212.207.80	147.237.76.197	India	e.hinush.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.77.205	United Kingdom	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
128.232.110.28	147.237.72.167	United Kingdom	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
121.46.107.14	147.237.76.44	India	e.refuah.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
91.201.236.158	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.158	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
77.252.26.51	147.237.77.61	Poland	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
66.249.73.171	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
66.249.64.105	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
163.172.129.15	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
128.232.110.28	147.237.76.199	United Kingdom	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.225.228	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	371
8.37.225.228	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	67
77.127.22.57	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	46
77.127.22.57	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	46
77.127.22.57	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	26
109.253.139.246	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	18
109.253.139.246	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
46.19.86.88	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
109.253.131.105	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
109.64.182.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
109.64.182.74	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.11	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.56.122	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.142.4.63	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
176.13.246.140	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
84.108.236.253	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.30.245	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
131.253.25.167	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.64.124.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
176.13.7.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.48	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
37.46.38.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
85.64.124.34	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.48	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
81.218.208.175	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
176.13.7.22	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
109.253.244.246	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.22.221	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.7.22	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
176.13.16.213	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.53	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
77.125.7.150	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
85.64.124.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.85.48	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.142.4.63	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
24.187.165.214	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
77.125.22.221	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
85.130.217.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.142.4.63	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.85.83	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
187.61.110.201	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	128
2.53.7.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	76
46.19.85.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
46.19.85.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
109.253.146.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
166.137.14.49	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	2
37.26.148.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.40.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.76.72	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/assetlinks.json	Block	1
77.139.56.173	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
31.154.81.76	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
109.253.139.246	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/intemational_training	Block	1
46.19.86.11	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
176.13.18.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
77.139.132.129	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.240.192.138	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/robots.txt	Block	1
31.154.81.76	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.106	Block	1
178.63.101.134	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/pratim/pirteychayal/	Block	1
80.179.122.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/3156.jpg	Block	1
117.200.13.164	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/true	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1153-he/chinuch.aspx	Block	1
46.120.68.27	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
212.76.117.23	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
84.109.4.76	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.69.110	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/iturim/asp/displayallsoldiers.asp	Block	1
157.55.39.125	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
77.139.40.218	France	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
46.120.68.27	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
24.187.165.214	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
85.65.25.220	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceholder\$questionUpdate\$txtOtherQuestion in www.aka.idf.il/main/giyus/faq.aspx	None	1