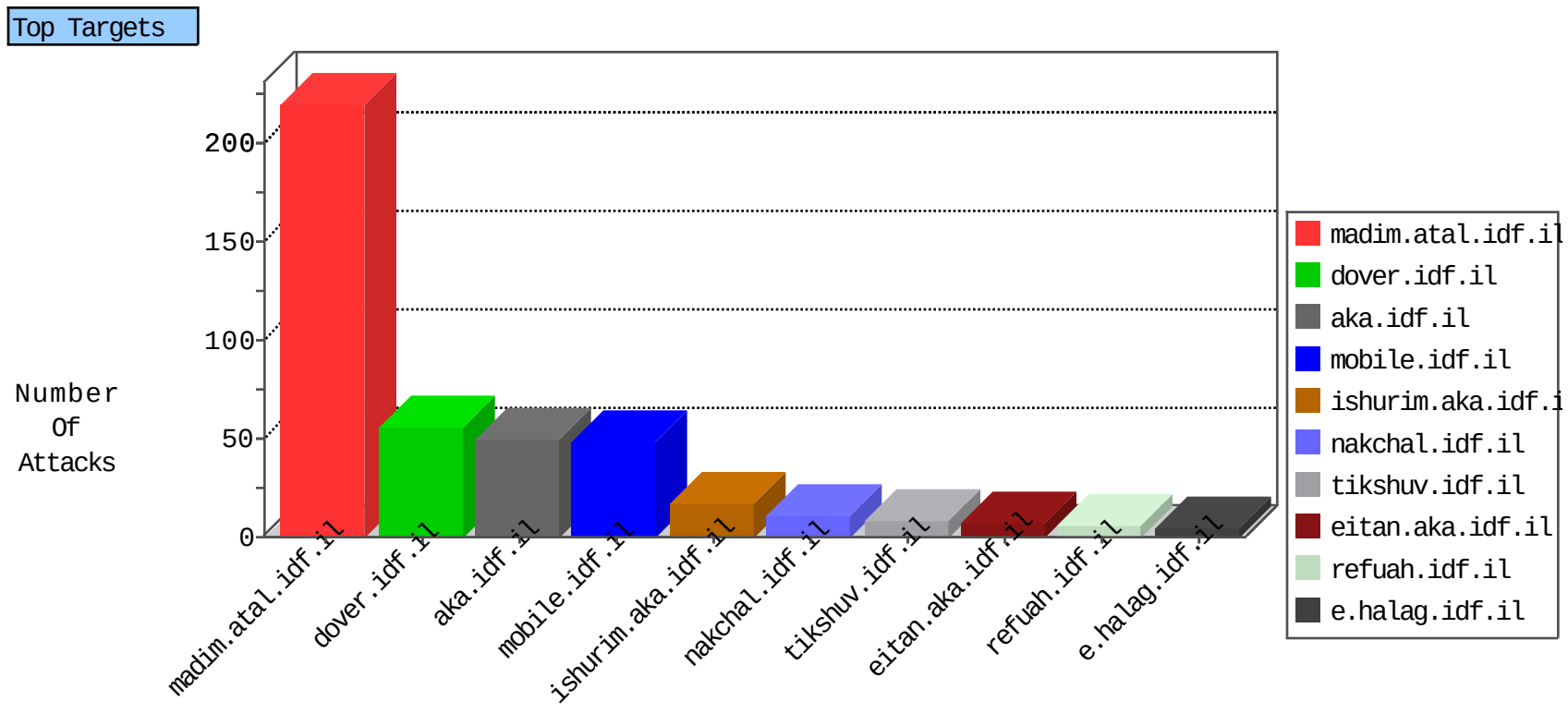
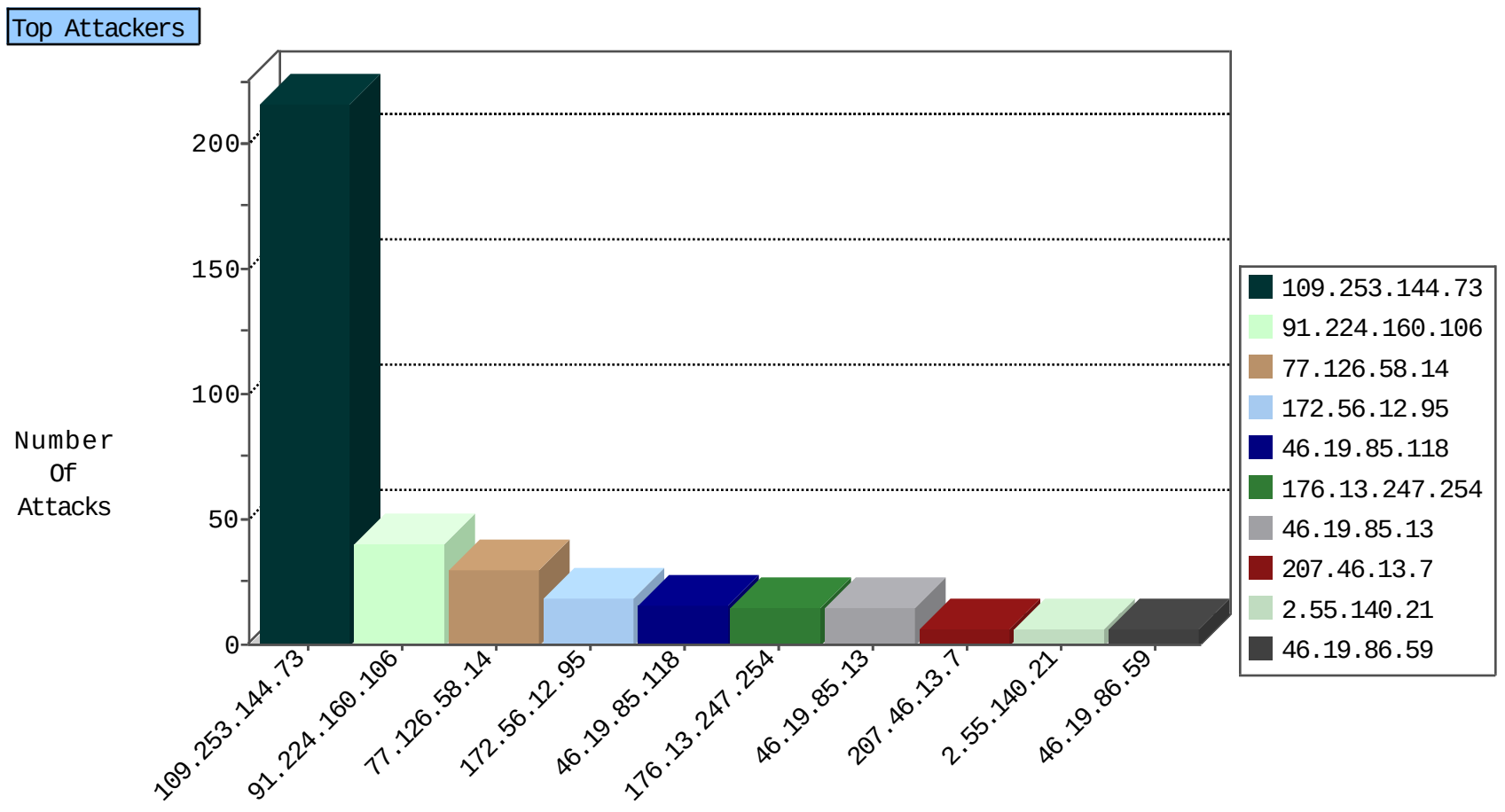
09-19-2016-06:04:04 to 09-19-2016-07:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-19-2016-06:04:04 to 09-19-2016-07:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
129.97.74.14	Canada	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	2
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
142.54.174.84	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
208.110.84.69	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
63.141.231.195	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	1
204.12.220.82	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	1
157.55.39.98	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.204.224.235	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	1
69.30.193.252	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
173.208.197.202	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.204.224.235	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
91.224.160.106	Netherlands	147.237.77.178	e.matpash.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
208.110.84.68	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
173.208.197.202	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	1
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-19-2016-06:04:04 to 09-19-2016-07:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-19-2016-06:04:04 to 09-19-2016-07:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.224.160.106	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	3
91.224.160.106	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
91.224.160.106	147.237.76.201	Netherlands	e.atal.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	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
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	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
78.128.80.33	147.237.77.121	Bulgaria	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
201.132.203.154	147.237.76.202	Mexico	e.halag.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
123.56.190.151	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.38	Netherlands	e.e.meitav.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	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.196	Netherlands	e.sviva.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
91.224.160.106	147.237.76.176	Netherlands	test.ncore.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
188.138.56.180	147.237.77.243	Germany	mobile.idf.il	ET SCAN Potential SSH Scan	1
116.71.128.85	147.237.77.227	Pakistan	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

09-19-2016-06:04:04 to 09-19-2016-07:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
172.56.12.95	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
176.13.247.254	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	13
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.118	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.55.140.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.7	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
176.13.242.224	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
201.132.203.154	Mexico	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
79.178.249.15	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.118	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
213.57.38.50	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
80.246.130.157	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
46.19.85.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.65.12	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.59	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.59	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
64.134.232.171	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.98	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.237.138.202	Czech Republic	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
66.102.6.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.247.254	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.62.63	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
2.53.62.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
68.180.229.110	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
45.32.186.11	Netherlands	147.237.0.35	akaws.idf.il	drop		drop	1
85.64.35.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
115.188.73.165	New Zealand	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
2.55.134.73	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
80.246.130.155	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
72.176.162.218	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
185.3.147.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
45.32.186.11	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
85.248.227.164	Slovakia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
2.53.4.37	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
120.132.68.33	China	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.15	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
89.248.172.16	Netherlands	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
2.53.55.2	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
79.176.81.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
66.102.6.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.214	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-19-2016-06:04:04 to 09-19-2016-07:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.144.73	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	216
80.246.138.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.19.223	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
77.138.108.40	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
141.226.148.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	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
80.246.130.157	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.65.10	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/assetlinks.json	Block	1
207.46.13.30	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
68.180.228.159	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.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
138.201.30.66	Germany	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1

09-19-2016-06:04:04 to 09-19-2016-07:04:04