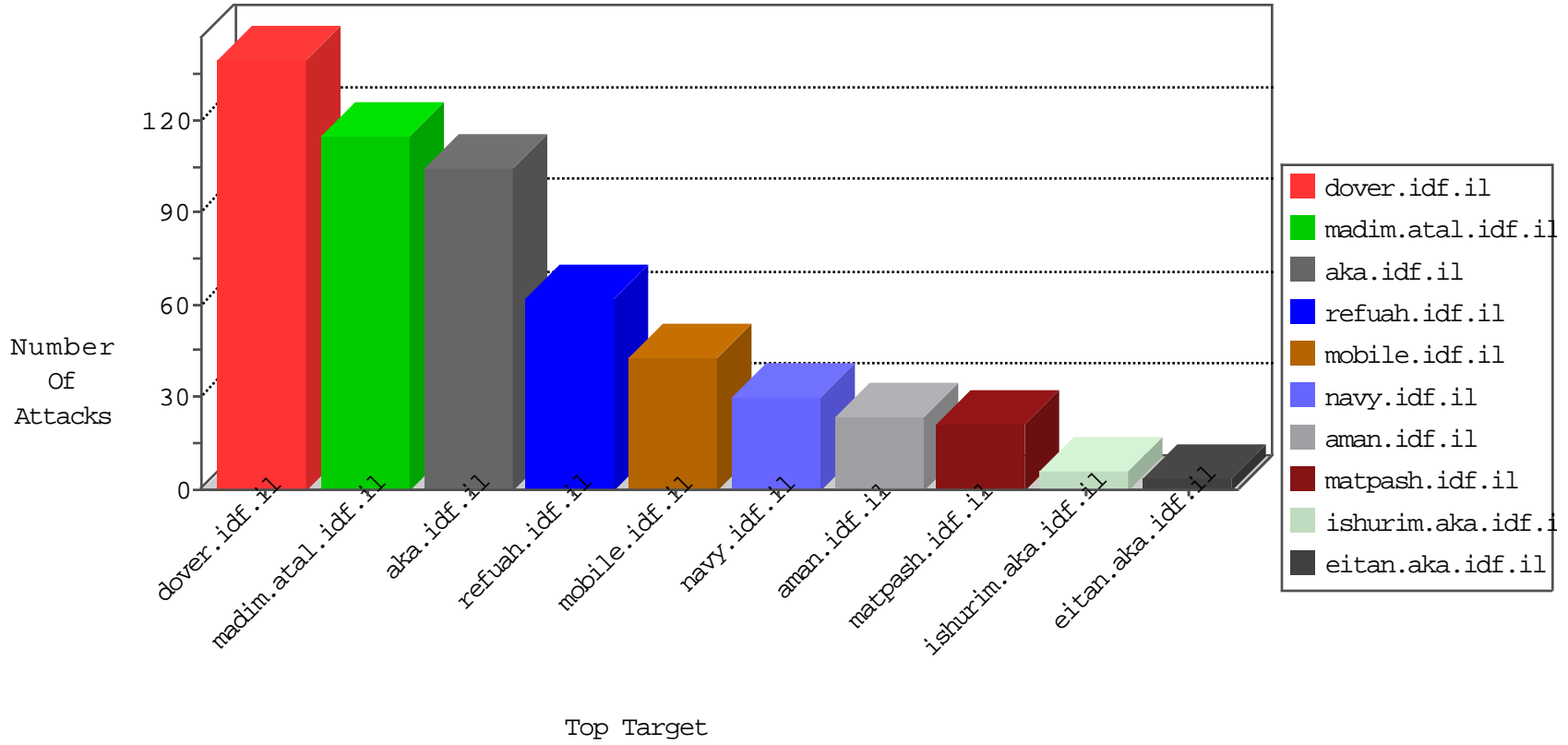


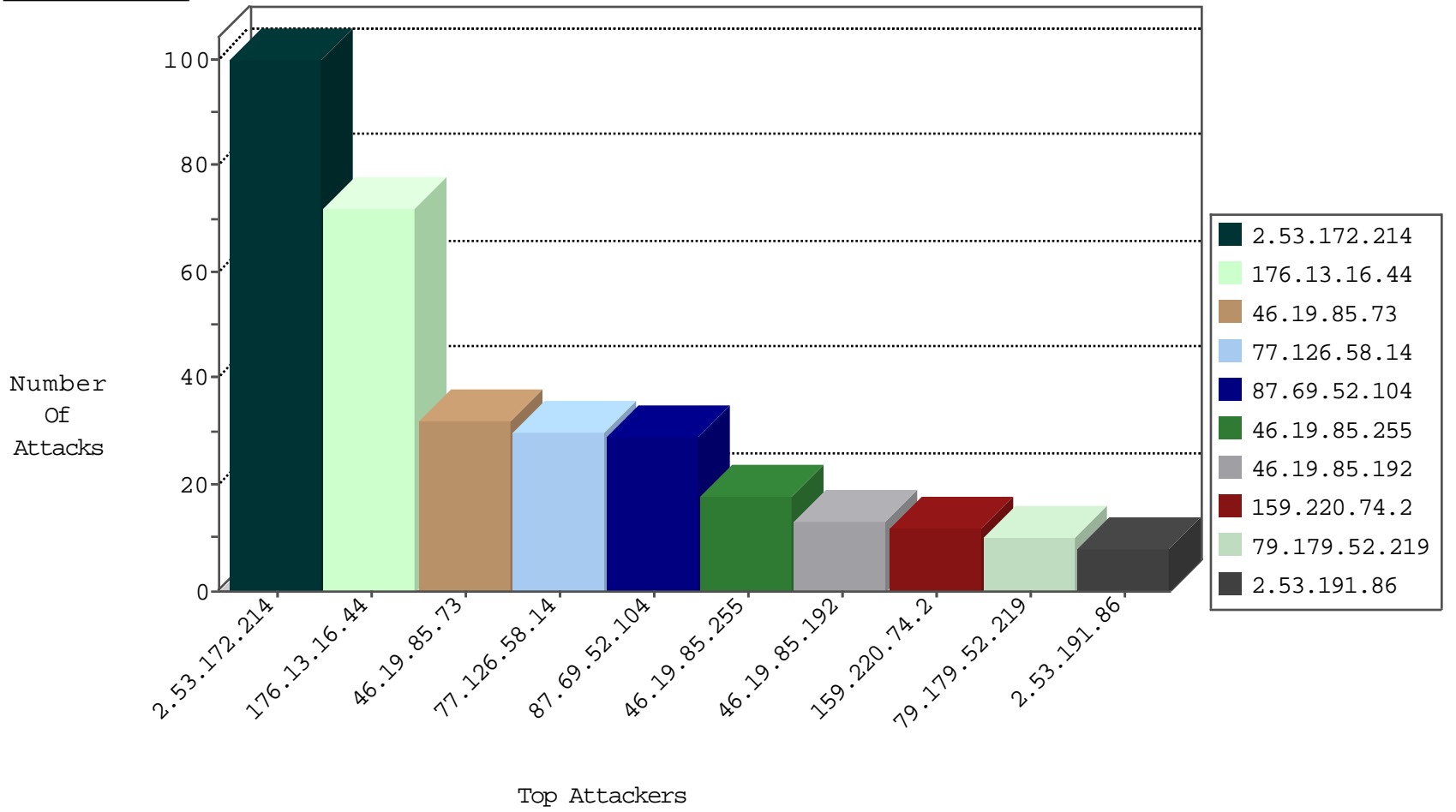
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	7
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
156.56.250.226	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	2
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
139.78.141.243	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	2
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
160.80.221.37	Italy	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
58.242.248.5	China	147.237.72.14	dover.idf.il(old)	JLM_Purple_Con_Limit_Tcp	drop	1
141.22.213.34	Germany	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
165.242.90.128	Japan	147.237.72.167	ishurim.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
58.242.248.5	China	147.237.76.196	e.sviva.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.212.113.178	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
193.1.13.12	Ireland	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.234.159.250	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.94.96.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.242.248.5	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
58.242.248.5	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
217.69.133.221	147.237.72.166	Russian Federation	aka.idf.il	WEB-CGI redirect access	1
5.255.90.133	147.237.0.16	Netherlands	ny-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
202.155.58.28	147.237.0.15	Indonesia	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.228	147.237.76.198	Switzerland	e.ychalan.idf.il	ET SCAN Potential SSH Scan	1
101.66.59.151	147.237.77.235	China	sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.50	147.237.76.148	Ukraine	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.106.103	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
66.249.69.160	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
58.242.248.5	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.116.166.10	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
185.129.148.230	147.237.77.170	Latvia	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.228	147.237.0.200	Switzerland	m4u.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.76.148	Ukraine	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
85.93.5.68	147.237.76.31	United Arab Emirates	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
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
176.13.16.44	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	20
176.13.16.44	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
176.13.16.44	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	18
87.69.52.104	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
159.220.74.2	United Kingdom	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.53.133.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.85.73	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.73	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
87.69.52.104	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
79.180.82.5	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
2.55.12.228	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.69.52.104	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.255	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.255	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.52.219	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.179.52.219	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
2.53.191.86	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
85.250.94.128	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.26.180.41	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
176.13.16.44	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
176.13.16.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
157.55.39.106	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.116.175.102	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
176.13.16.44	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
2.53.191.86	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
185.32.179.138	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.255	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
157.55.39.103	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.148.244	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
176.13.235.130	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
176.13.16.44	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
89.138.115.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
141.226.217.239	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.162	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.0.124	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
185.120.124.20	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
37.46.38.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.66.148.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
109.186.88.56	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.46.41.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
159.220.74.2	United Kingdom	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.172.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	100
109.66.115.4	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.66.115.4	Block	4
46.19.86.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.208.38	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/gyus/miyun/miyunderugshikulim.aspx	Block	3
109.253.213.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.102.242.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.21.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.7.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.64.228.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.142.46	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
217.69.133.221	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/redirects/ssl-redirect.html	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
176.228.219.58	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
77.139.208.38	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.208.38	Block	1
109.66.115.4	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/miyun/miyunlobby.aspx	Block	1
185.27.106.55	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/gyus/authenticationervice.asmx/getauthuser	Block	1
2.55.12.228	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	1
188.120.154.99	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
84.109.102.53	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/	Block	1
213.8.204.56	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
37.26.147.248	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1