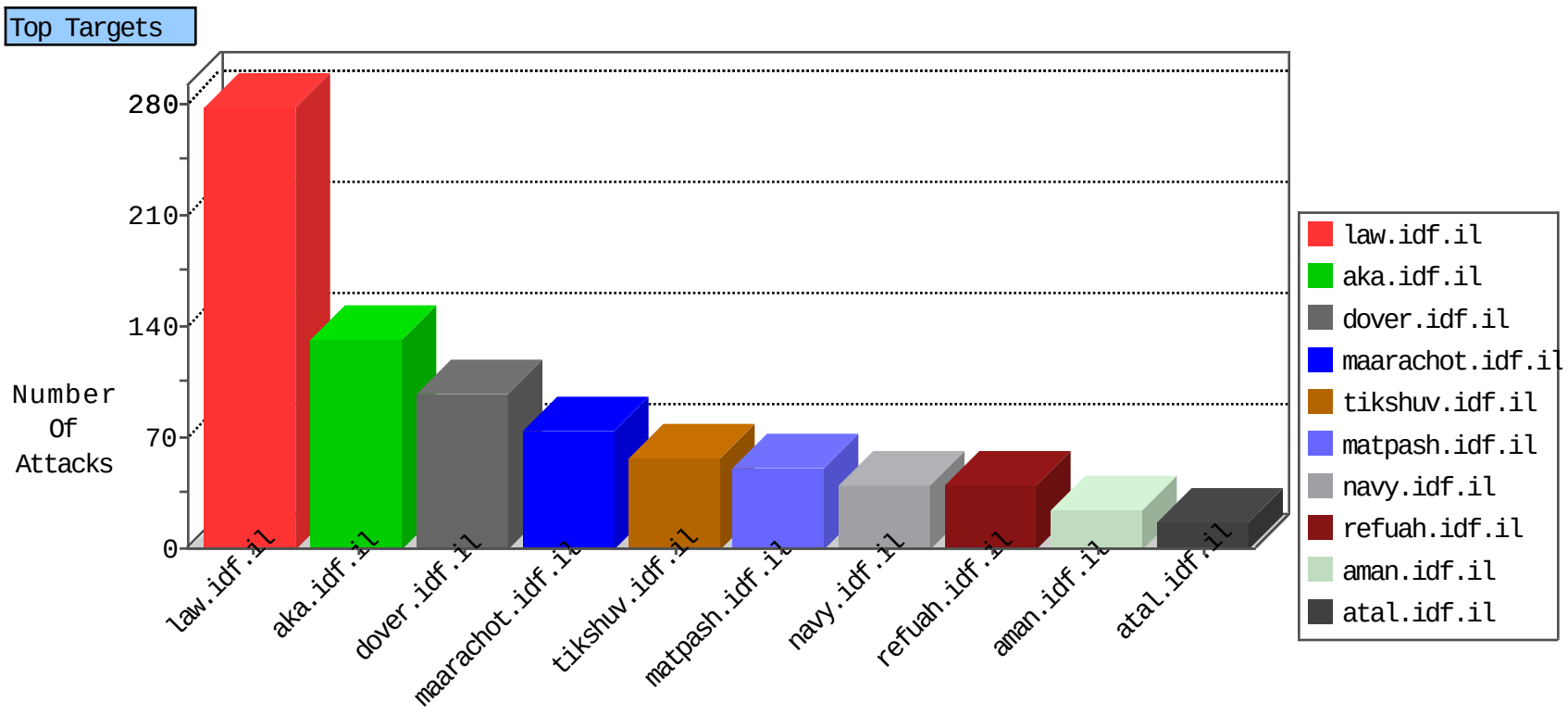
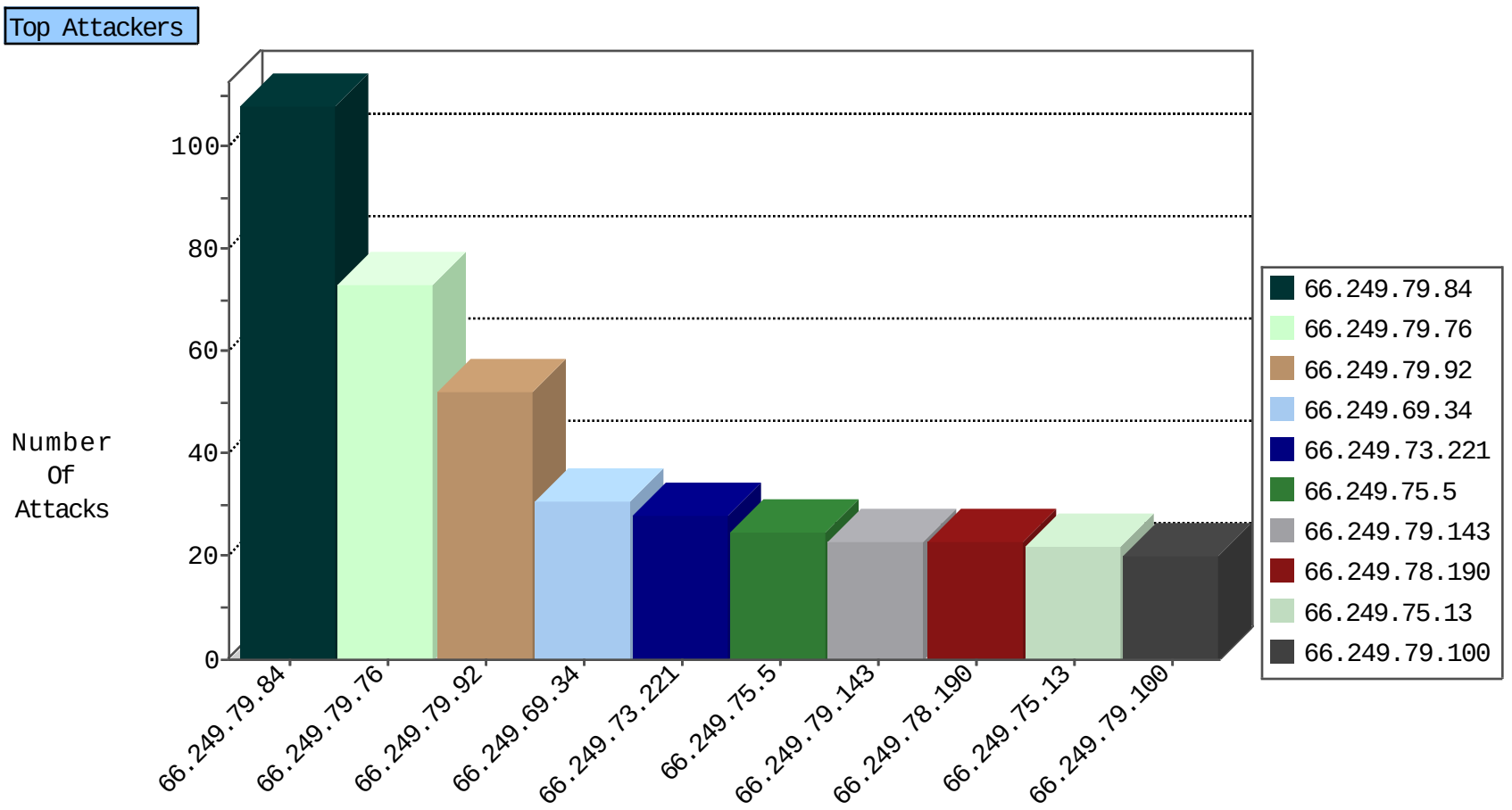
04-03-2015-05:03:04 to 04-03-2015-06:03:04

IDF Under Attack
04-03-2015-05:03:04

Top Targets



Top Attackers



04-03-2015-05:03:04 to 04-03-2015-06:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.79.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	108
66.249.79.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	73
46.19.86.41	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
66.249.79.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	52
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	31
66.249.73.221	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	28
66.249.75.5	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	25
66.249.79.143	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	23
66.249.75.13	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	22
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	22
66.249.79.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	20
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	16
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	15
66.249.79.151	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	15
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	15
66.249.79.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	14
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	14
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	14
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	12
66.249.75.64	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	11
66.249.75.117	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.79.159	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	11
66.249.79.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.75.80	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	11
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	9
66.249.78.54	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	8
66.249.64.14	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	8
66.249.73.237	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	8
66.249.75.72	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	7
66.249.64.27	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	7
66.249.64.10	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.79.113	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	6
66.249.64.19	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	6
66.249.80.75	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
66.249.64.151	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	6
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
66.249.78.191	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	5
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
66.249.78.215	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ip_Web_In	drop	4
66.249.78.248	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	4
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	4
66.249.64.147	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	4
66.249.92.51	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
66.249.92.57	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
66.249.78.44	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	3
66.249.78.184	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	3

04-03-2015-05:03:04 to 04-03-2015-06:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
66.240.192.138	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
156.111.111.155	United States	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-03-2015-05:03:04 to 04-03-2015-06:03:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
43.255.191.161	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
117.135.163.104	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.161	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
89.248.162.228	Netherlands	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
208.39.68.33	United States	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.161	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
203.114.104.30	Thailand	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.161	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
203.114.104.30	Thailand	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.161	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
177.129.79.177	Brazil	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
117.135.163.104	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
208.39.68.33	United States	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
203.114.104.30	Thailand	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.161	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1

04-03-2015-05:03:04 to 04-03-2015-06:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	8
183.11.80.131	China	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	7
111.206.36.133	China	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
41.37.121.57	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
70.209.134.159	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.60	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
155.94.254.133		147.237.76.147	chinuch.aka.idf.il		drop	drop	2
70.209.134.159	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
183.11.80.131	China	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
122.107.249.146	Australia	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
46.19.85.60	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
70.209.134.159	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
122.107.249.146	Australia	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
74.82.47.31	United States	147.237.76.34	yohalan.idf.il		drop	drop	1
64.125.239.22	United States	147.237.76.201	e.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
188.165.15.198	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.198	Block	4
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
181.165.108.2	Argentina	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	2
207.46.13.16	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.16	Block	1
93.172.144.140	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
63.141.204.13	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
77.127.192.171	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Unknown Parameter pageNum in www.aka.idf.il/chinuch/faq/default.asp	None	1
99.238.150.210	Canada	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$txtMisparIshi in www.aka.idf.il/main/sachar/	None	1
192.99.15.227	Canada	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
79.180.33.97	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
210.48.94.145	New Zealand	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
109.226.17.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
203.133.169.157	Korea, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 203.133.169.157	Block	1
81.144.138.34	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.144.138.34	Block	1
213.57.156.145	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
157.55.39.19	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/901-9135-he/cogat.aspx	Block	1
203.133.169.157	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/110503-2.stm	Block	1
89.248.172.57	Netherlands	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
217.115.112.107	Ireland	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
74.82.47.3	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1