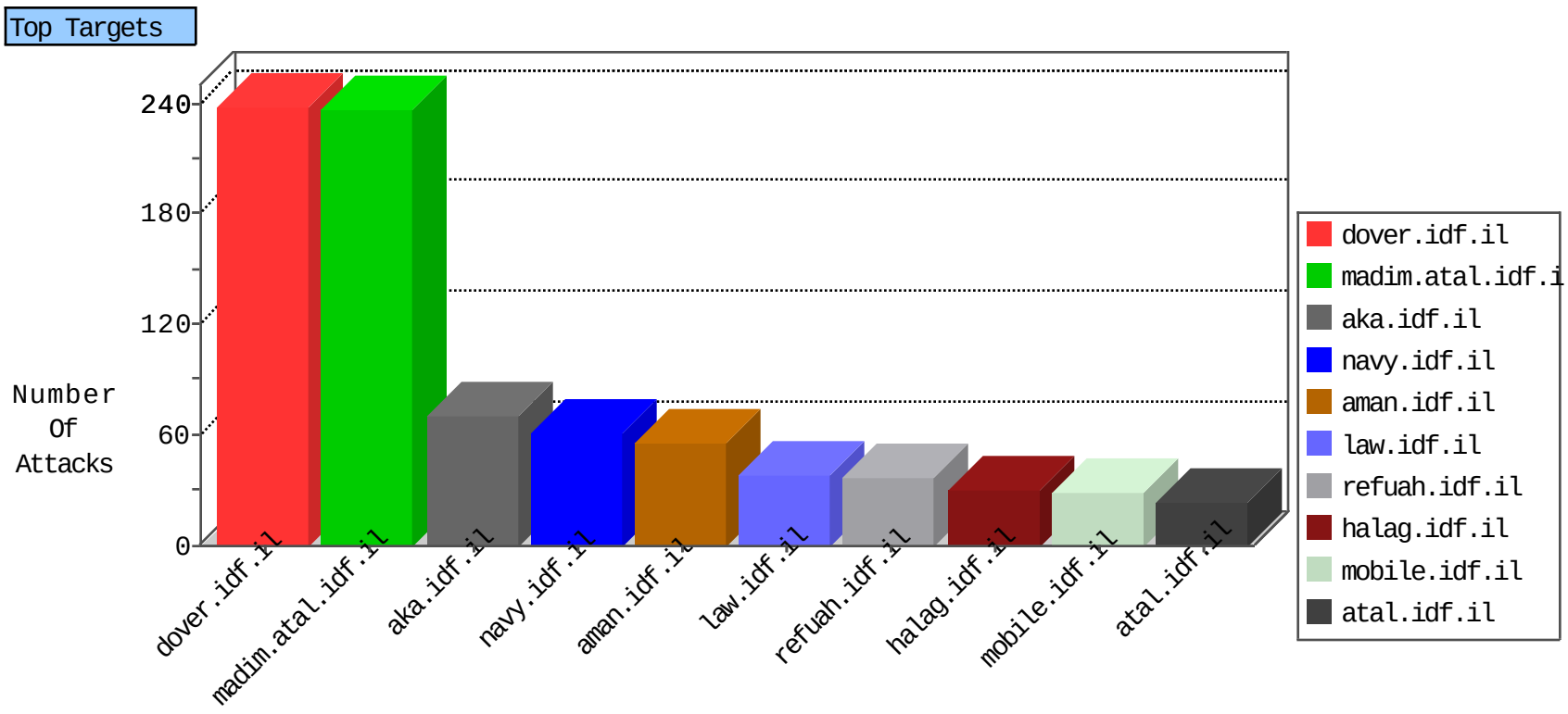
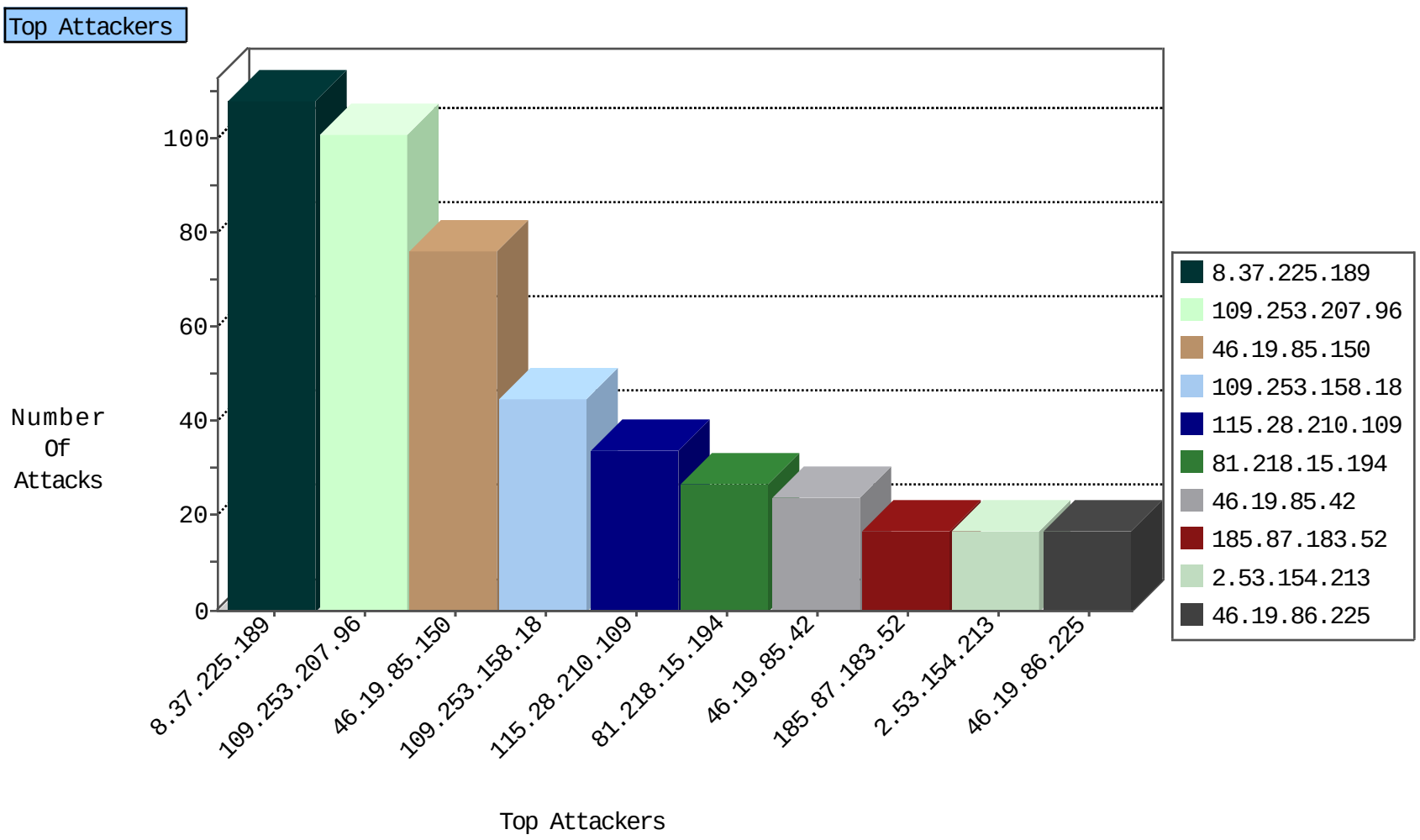
09-09-2016-15:04:04 to 09-09-2016-16:04:04

IDF Under Attack Daily Report





09-09-2016-15:04:04 to 09-09-2016-16:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.225.189	United States	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	10
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
8.37.225.189	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
8.37.225.189	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
207.46.13.93	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
212.179.90.106	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
123.59.59.52	China	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
185.94.111.1	Russian Federation	147.237.76.202	e.halag.idf.il	Black List	drop	1

09-09-2016-15:04:04 to 09-09-2016-16:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.91.49.78	United States	147.237.77.74	law.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	10
54.86.105.62	United States	147.237.77.74	law.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	10
52.23.198.65	United States	147.237.77.74	law.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	5
46.19.85.179	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-09-2016-15:04:04 to 09-09-2016-16:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.179.38.41	147.237.76.42	Israel	refuah.idf.il	ET SCAN NMAP -sA (2)	7
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
104.232.98.38	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
93.174.94.142	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.201.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.6	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	1
50.116.123.135	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
37.163.244.255	147.237.72.166	France	aka.idf.il	ET SCAN NMAP -sA (2)	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
190.66.172.128	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.232.98.38	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
104.232.98.38	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
93.174.94.142	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
63.142.161.5	147.237.76.201	Canada	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
211.141.78.56	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.129.15	147.237.77.74	United Kingdom	law.idf.il	ET SCAN NMAP -sS window 1024	1

09-09-2016-15:04:04 to 09-09-2016-16:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
8.37.225.189	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
8.37.225.189	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	48
81.218.15.194	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
2.53.154.213	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	17
46.121.195.125	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
115.28.210.109	China	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.86.24	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	12
37.26.149.226	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
115.28.210.109	China	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	9
115.28.210.109	China	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	8
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.210.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.75.129	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.66.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.42	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.36.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.42	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.64.39.127	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
77.127.32.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.64.39.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
89.237.121.61	France	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.117.221.57	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.225	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
83.244.113.226	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
176.13.5.242	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	4
63.142.161.5	Canada	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
5.102.242.119	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
154.127.78.58	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.120.125.111	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.209	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.30.25.69	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.135	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.240	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
157.55.39.202	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.27.186	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.15	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.56.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
85.130.129.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.76.104.3	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
85.130.129.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

09-09-2016-15:04:04 to 09-09-2016-16:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.207.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	101
46.19.85.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	76
109.253.158.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
2.55.21.168	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.55.21.168	Block	8
79.181.233.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
77.126.18.205	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
2.55.21.168	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
93.173.16.7	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
80.246.136.81	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.0.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.57.144.9	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
89.248.172.16	Netherlands	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/robots.txt	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/70023.doc	Block	1
77.138.198.47	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx	Block	1
46.117.97.244	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.253.210.43	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
109.66.141.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl37 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
77.139.74.137	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/edim/theproj/theproj.asp	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
144.76.16.162	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/brothers/skira/default.asp	Block	1
81.218.15.194	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.76.102	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
77.139.222.187	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
46.121.195.125	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
85.64.116.166	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
68.180.228.162	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
37.142.1.179	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	1
109.253.193.128	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.177.31.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.66.30	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/8/1298.pdf	Block	1

09-09-2016-15:04:04 to 09-09-2016-16:04:04