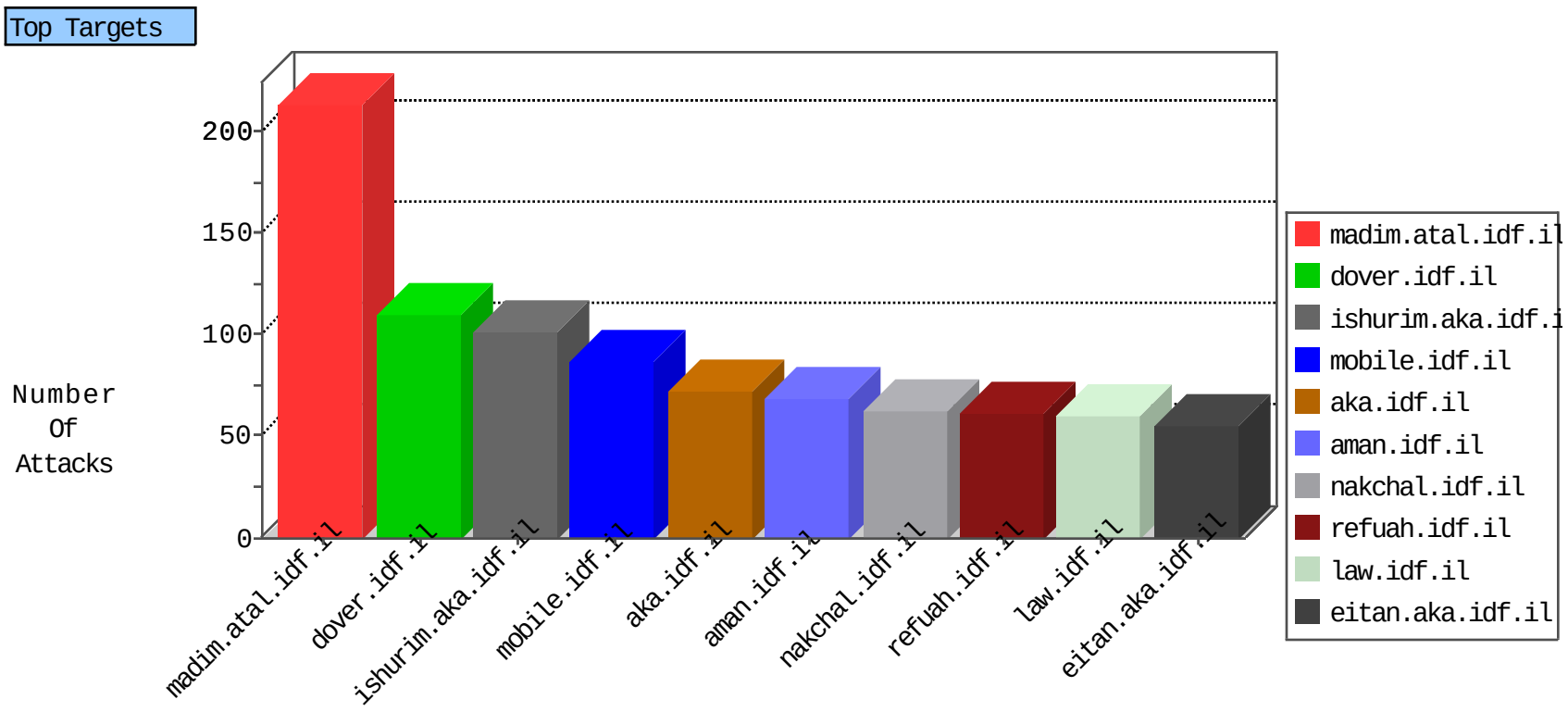
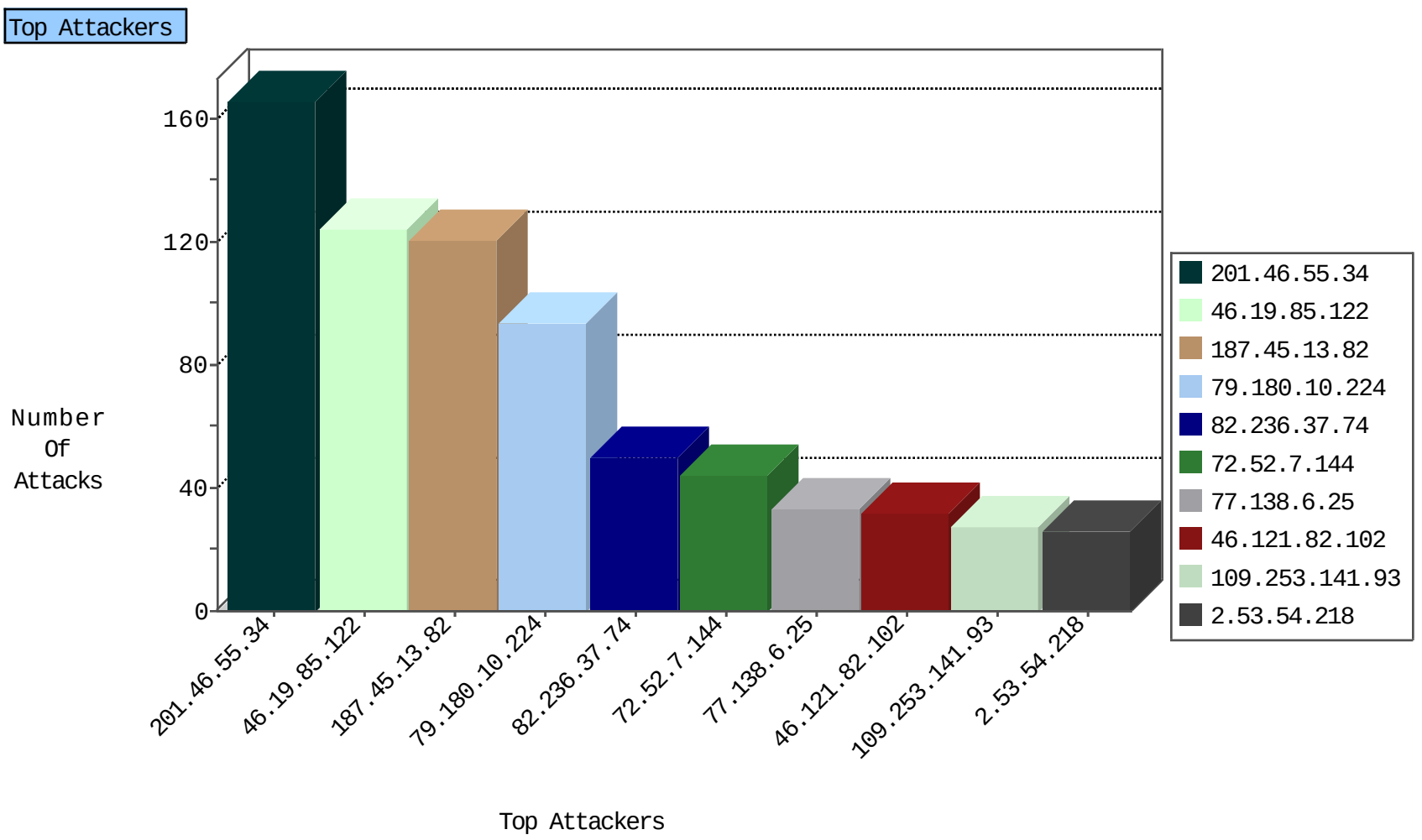
09-10-2016-16:04:00 to 09-10-2016-17:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-10-2016-16:04:00 to 09-10-2016-17:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.57.133.154	China	147.237.77.170	maarachot.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
149.202.89.123	France	147.237.76.34	yohalan.idf.il	Black List	drop	1
80.82.78.27	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
93.174.93.156	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1

09-10-2016-16:04:00 to 09-10-2016-17:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
75.134.133.243	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
75.134.133.243	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1

09-10-2016-16:04:00 to 09-10-2016-17:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
190.252.164.249	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.169.150	147.237.72.156	United Kingdom	aman.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.33.217	147.237.76.86	Israel	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
46.227.67.158	147.237.72.167	Sweden	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.48.93.217	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
23.239.31.132	147.237.77.234	United States	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
176.58.124.35	147.237.76.147	United Kingdom	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.237.146.151	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
47.90.22.46	147.237.0.19	Canada	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
37.48.93.217	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential SSH Scan	1
37.48.93.217	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1

09-10-2016-16:04:00 to 09-10-2016-17:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.180.10.224	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	92
46.121.82.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
2.53.54.218	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
187.45.13.82	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
187.45.13.82	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
187.45.13.82	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.34	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.45.13.82	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.34	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.45.13.82	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.45.13.82	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.45.13.82	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.34	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.34	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.34	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
201.46.55.34	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
201.46.55.34	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
85.64.116.79	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.117.250.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
201.46.55.34	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
31.154.81.16	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	10
84.109.153.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.149.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.116.82.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
138.134.192.10	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
5.28.183.251	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.81.16	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence		monitor	5
139.162.13.205	Singapore	147.237.0.16	my-kosher-kravi.idf.il	drop	SAM rule	drop	5
201.46.55.34	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.151	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.55.134.219	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.68	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.68	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
201.46.55.34	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
201.46.55.34	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
201.46.55.34	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.53.157.88	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
201.46.55.34	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
82.114.168.157	Yemen	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
201.46.55.34	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
201.46.55.34	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
82.114.168.157	Yemen	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
201.46.55.34	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
201.46.55.34	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
31.154.81.16	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
201.46.55.34	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
201.46.55.34	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
82.166.235.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
77.138.194.163	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4

09-10-2016-16:04:00 to 09-10-2016-17:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	124
77.138.6.25	France	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
109.253.141.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
82.236.37.74	France	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	25
46.121.252.215	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	18
85.250.238.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
82.236.37.74	France	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 82.236.37.74	Block	14
82.236.37.74	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/	Block	11
84.111.241.194	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	8
109.66.126.123	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	7
2.53.54.218	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
46.120.36.19	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
46.121.82.102	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
213.8.204.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.149.157	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
5.254.65.26	Turkey	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
93.173.19.17	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
79.180.241.224	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1072-he/nakhal.aspx	Block	1
66.249.64.220	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
31.154.81.14	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
85.64.116.79	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized Method POST for www.eitan.aka.idf.il/1105-he/contactus.aspx	None	1
77.138.236.38	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.236.38	Block	1
66.249.64.228	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/992-he/patzar.aspx	Block	1
37.26.147.150	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
85.64.247.51	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
77.138.236.38	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
46.121.40.183	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
109.66.135.122	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
2.53.157.88	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	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/7/61267.gif	Block	1
85.250.120.7	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
79.176.82.230	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
68.180.229.181	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
37.142.3.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.180.10.224	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/1044-he/homepage.asp	Block	1

09-10-2016-16:04:00 to 09-10-2016-17:04:00