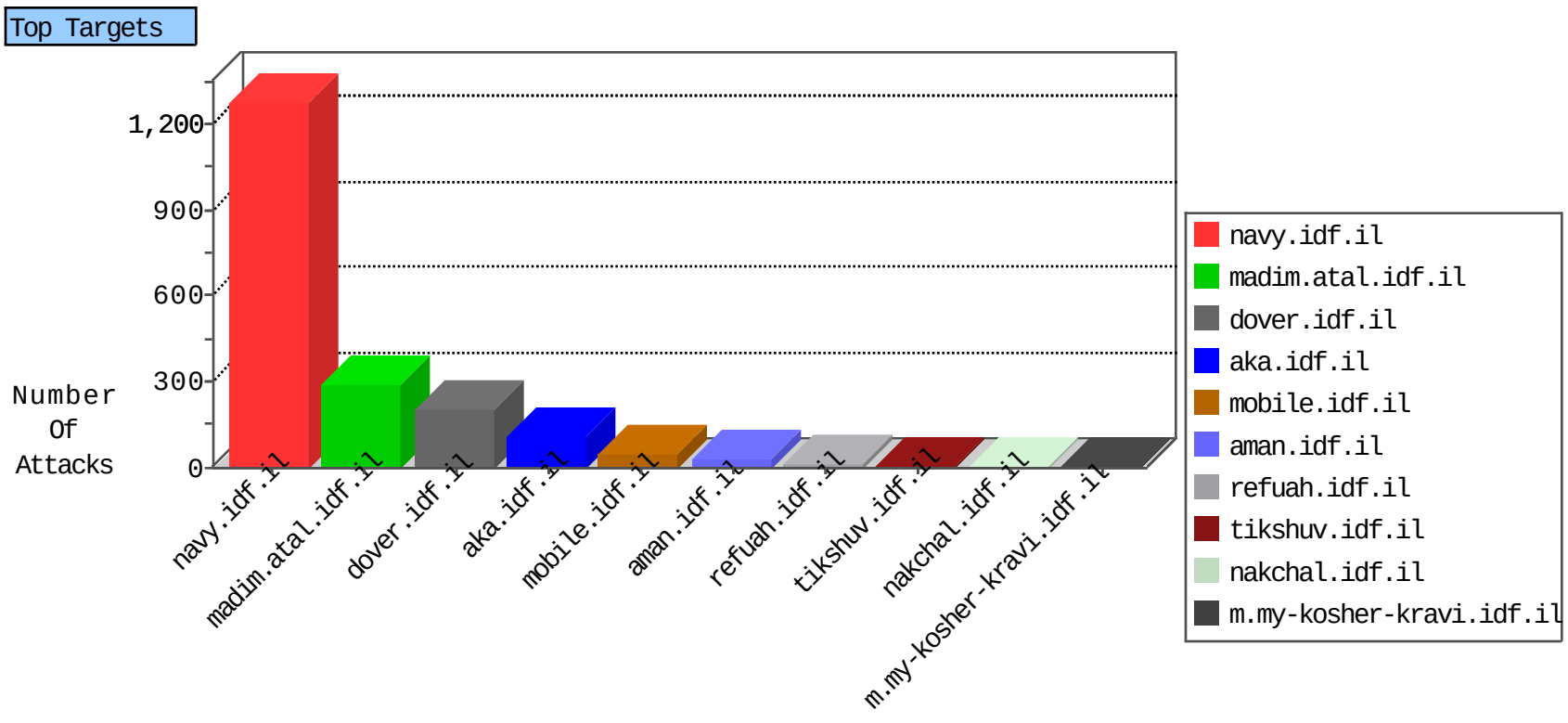
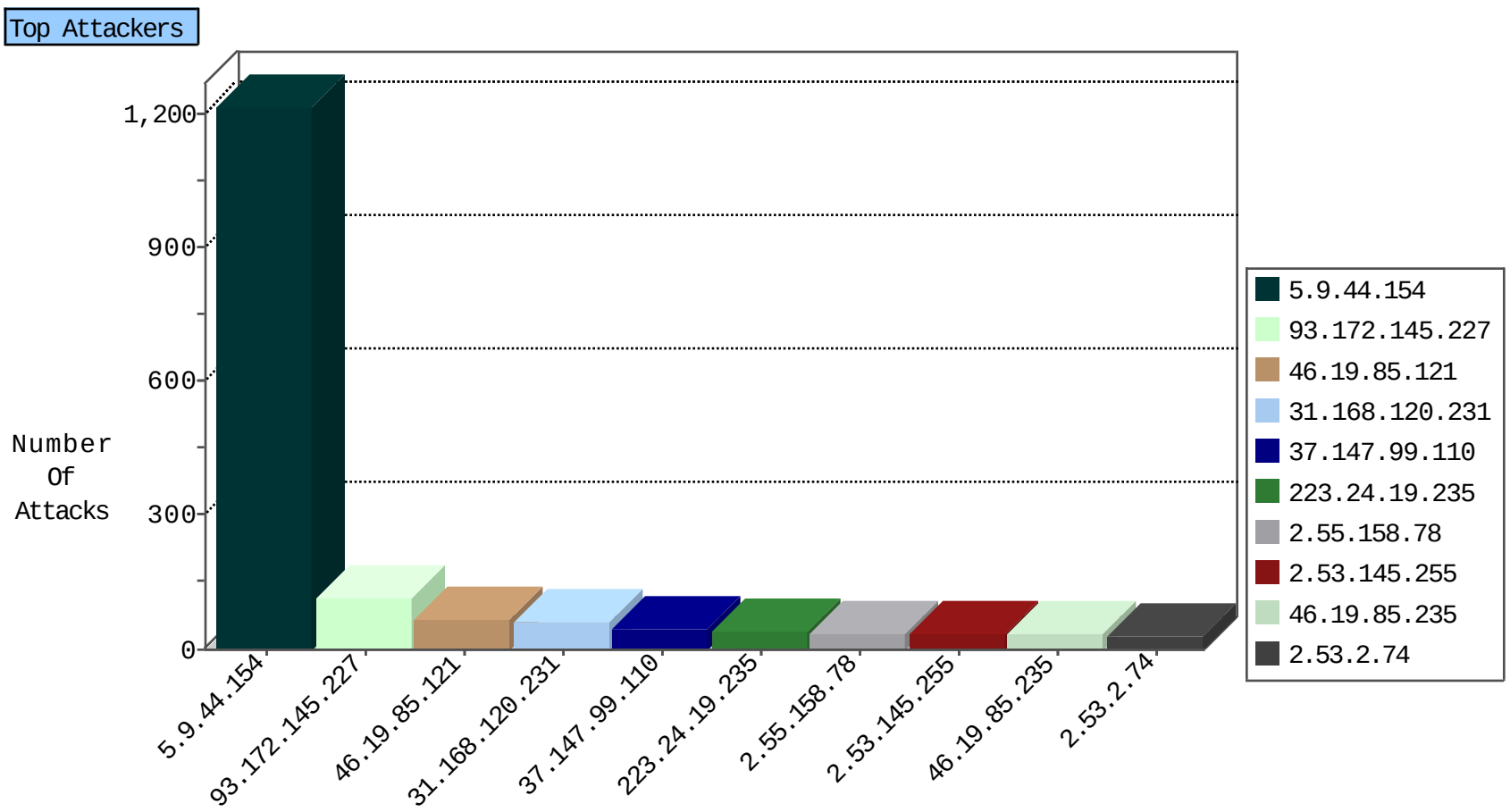
09-22-2016-20:04:02 to 09-22-2016-21:04:02

IDF Under Attack Daily Report



Top Target



Top Attackers

09-22-2016-20:04:02 to 09-22-2016-21:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.89.150	Israel	147.237.72.166	aka.idf.il	Black List	drop	4
183.60.48.25	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
213.8.204.1	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-22-2016-20:04:02 to 09-22-2016-21:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2

09-22-2016-20:04:02 to 09-22-2016-21:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
106.120.209.148	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
87.68.23.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.113	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
14.184.152.166	147.237.0.17	Vietnam	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.205.151.197	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
211.149.201.80	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.37	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
139.162.187.89	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
106.120.209.148	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -f -sS	1
85.250.105.91	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
40.114.15.49	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
218.205.151.197	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -f -sS	1
206.246.150.226	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.37	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1

09-22-2016-20:04:02 to 09-22-2016-21:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1208
37.147.99.110	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
223.24.19.235	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
2.55.158.78	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
2.55.158.78	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
46.19.85.235	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
2.53.145.255	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.145.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.53.2.74	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
2.53.2.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
46.19.85.235	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.53.2.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
128.69.210.181	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.235	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.86.188	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.112	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.53.145.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.112	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.53.145.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.53.145.255	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
79.178.254.141	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.178.254.141	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.53.16.19	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
193.19.167.227	Poland	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
79.178.254.141	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
193.19.167.227	Poland	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
31.168.152.111	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
85.64.124.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.112	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.26.146.164	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
141.226.218.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.242.116.101	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.180.169.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
193.19.167.227	Poland	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
213.8.204.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.167	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
31.25.78.33	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
79.178.188.52	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
193.19.167.227	Poland	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
213.151.49.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.111.102.3	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.167	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.55.158.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.43.181.159	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
77.138.231.243	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.138.88.205	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.250.75.153	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.253.156.164	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

09-22-2016-20:04:02 to 09-22-2016-21:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.172.145.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	115
46.19.85.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
31.168.120.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
46.19.85.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
37.26.146.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
5.102.254.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.111.172.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.6.27	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
185.32.179.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.117.75.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
46.117.120.45	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	1
187.161.242.184	Mexico	147.237.0.19	madim.atal.idf.il	Redundant HTTP Headers Content-Type	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
213.8.204.20	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Malformed URL http/1.1	Block	1
2.53.54.167	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
109.160.213.168	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1437-he/atal.aspx	Block	1
77.138.96.96	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/syyarot/	Block	1
46.149.82.236	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	1
189.218.118.224	Mexico	147.237.0.17	m.my-kosher-kravi.idf.il	Redundant HTTP Headers Content-Type	Block	1
89.237.89.56	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	1
66.249.64.113	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
213.8.204.20	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method g=he in URL www.idf.ilhttp/1.1	Block	1
176.13.247.217	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.149.82.236	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
201.172.236.225	Mexico	147.237.0.34	tikshuv.idf.il	Redundant HTTP Headers Content-Type	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.66.182	Block	1
46.116.219.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
24.46.146.24	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
77.139.137.139	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
66.102.9.30	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
201.175.113.125	Mexico	147.237.0.15	kosher-kravi.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
109.64.83.190	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
31.154.81.54	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
185.33.168.254	Palestinian Territory Occupied	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
79.177.210.191	Israel	147.237.72.167	ishurim.aka.idf.il	Double URL Encoding - parameter: rdfrom in www.ishurim.aka.idf.il/1050-he/pickcertificates.aspx	Block	1
66.240.192.138	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/robots.txt	Block	1
207.46.13.140	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
109.67.160.231	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-22-2016-20:04:02 to 09-22-2016-21:04:02