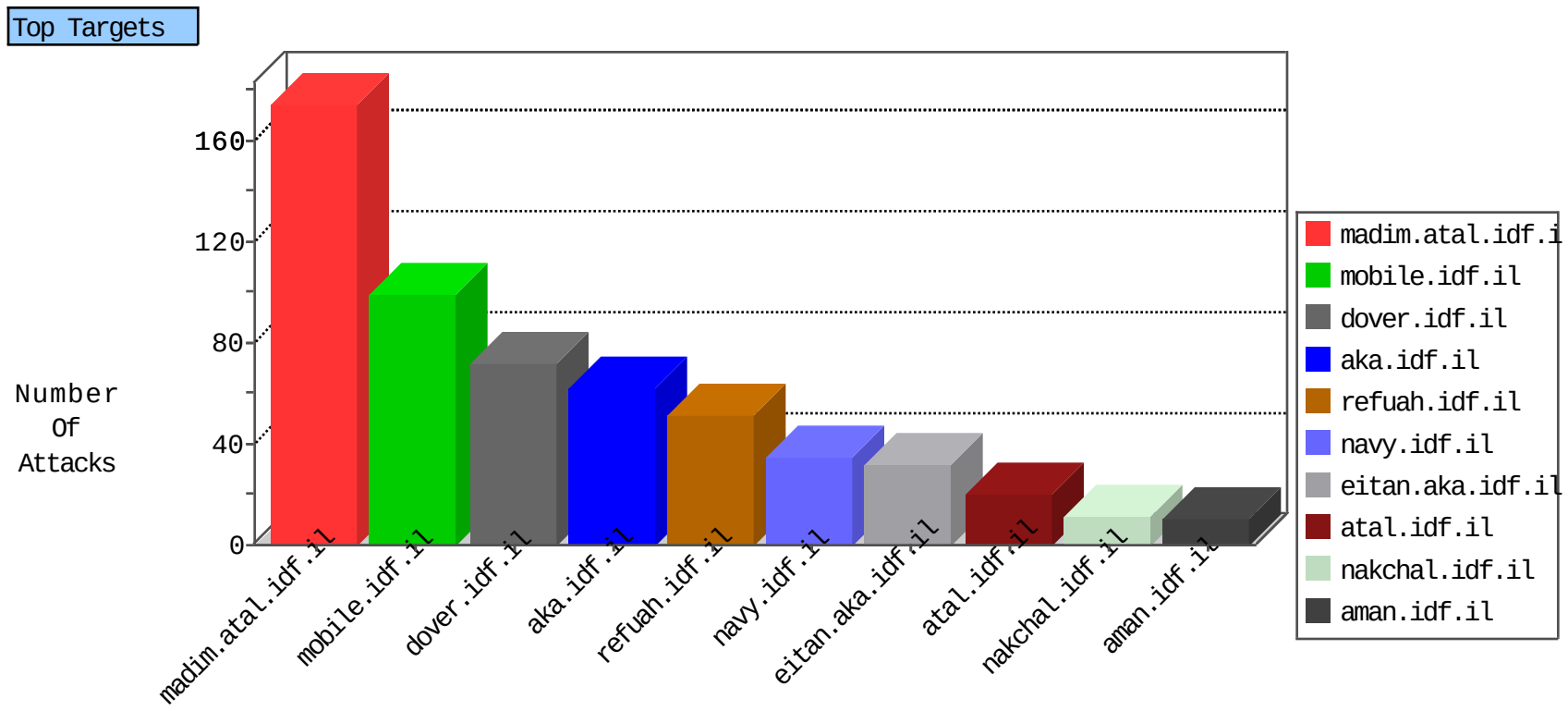
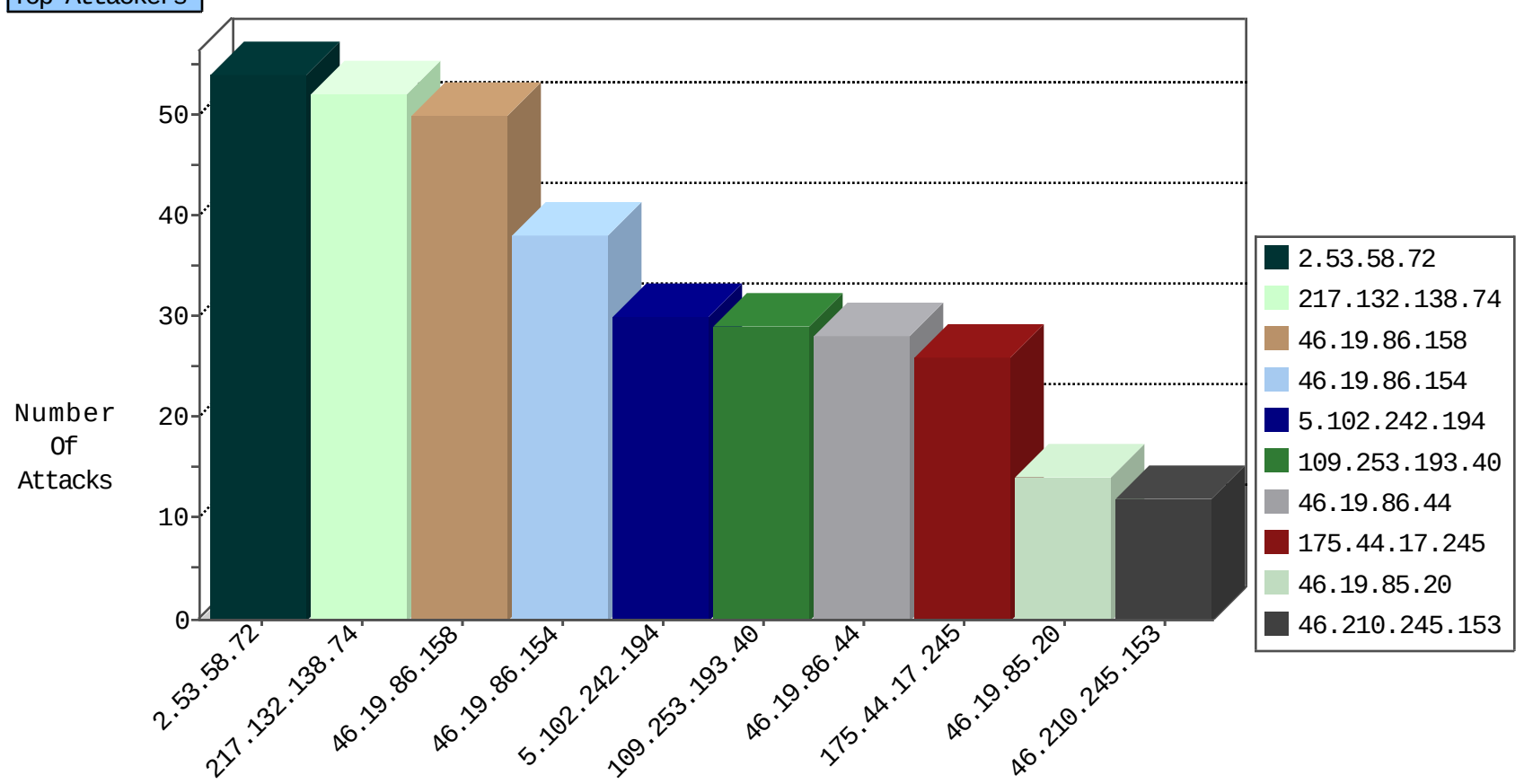
09-22-2016-23:04:02 to 09-23-2016-00:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-22-2016-23:04:02 to 09-23-2016-00:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.131.71	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
185.128.40.162	Switzerland	147.237.76.197	e.himush.idf.il	Black List	drop	1

09-22-2016-23:04:02 to 09-23-2016-00:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
88.237.197.9	Turkey	147.237.72.166	aka.idf.il	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1
188.165.250.173	France	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
46.183.222.176	Latvia	147.237.77.216	dover.idf.i	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
88.237.197.9	Turkey	147.237.72.166	aka.idf.il	C1000016: HTTP: administrator in URI	Permit	1

09-22-2016-23:04:02 to 09-23-2016-00:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
188.165.250.173	147.237.77.233	France	atal.idf.il	SQL Injection - Select From	8
79.177.227.200	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	3
200.58.214.138	147.237.76.197	Colombia	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.0.15	Cote D'Ivoire	kosher-kravi.idf.i	ET SCAN NMAP -sS window 4096	1
125.213.243.10	147.237.76.34	Thailand	yohalan.idf.il	ET SCAN Potential SSH Scan	1
116.71.128.85	147.237.76.34	Pakistan	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
104.167.6.84	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.222.5	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
200.58.214.138	147.237.77.74	Colombia	law.idf.il	ET SCAN NMAP -sS window 2048	1
52.144.44.251	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
200.58.214.138	147.237.76.197	Colombia	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
200.58.214.138	147.237.76.197	Colombia	e.himush.idf.il	ET SCAN NMAP -f -sS	1
196.47.173.21	147.237.0.15	Cote D'Ivoire	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
165.215.209.15	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
122.96.243.32	147.237.77.243	China	mobile.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.60.153.178	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.132.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
200.58.214.138	147.237.77.74	Colombia	law.idf.il	ET SCAN NMAP -sS window 4096	1
54.72.73.168	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
200.58.214.138	147.237.77.74	Colombia	law.idf.il	ET SCAN NMAP -f -sS	1

09-22-2016-23:04:02 to 09-23-2016-00:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
217.132.138.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
5.102.242.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.86.44	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.85.20	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.86.44	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
46.210.245.153	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
217.132.138.74	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
85.64.205.157	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
62.219.128.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
76.10.176.163	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
87.68.51.190	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
37.26.146.212	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
77.139.40.218	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.216	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
79.183.0.208	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
109.67.239.29	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
94.23.98.130	France	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
176.13.22.164	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.192.47	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
94.23.98.130	France	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
87.70.7.95	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.5	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.5	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
94.23.98.130	France	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
85.130.182.151	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
31.154.81.60	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
93.172.112.28	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
74.91.113.11	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
2.55.163.213	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.213	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
31.154.81.60	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
93.175.200.140	Ukraine	147.237.77.176	matpash.idf.il	Header Rejection	header rejection pattern found in request	monitor	2
46.19.86.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
74.91.113.11	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
68.180.228.44	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
31.154.81.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
74.91.113.11	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
79.181.186.196	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
109.253.134.226	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
74.91.113.11	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
2.53.1.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.72	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.66.177.48	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
74.91.113.11	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
187.198.134.107	Mexico	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
72.5.195.133	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
169.229.3.91	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.226.218.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

09-22-2016-23:04:02 to 09-23-2016-00:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.58.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
46.19.86.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
46.19.86.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
109.253.193.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
175.44.17.245	China	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 175.44.17.245	Block	17
79.177.172.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachr/	Block	6
175.44.17.245	China	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	6
217.132.138.74	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 217.132.138.74	Block	3
81.218.192.47	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
31.154.81.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
173.212.41.68	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/2392.jpg	Block	1
175.44.17.245	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/index.asp	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1379-21745-he/dover.aspx	Block	1
174.92.33.60	Canada	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
85.64.205.157	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.66.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
204.79.180.29	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/inner.asp	Block	1
169.229.3.91	United States	147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.180.228.99	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
87.68.51.190	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.66.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
2.53.41.236	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00_ctl00_ScriptManager1_HiddenField in www.aka.idf.il/main/giyus/	None	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
46.183.222.176	Latvia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/phppath/php	Block	1
109.66.177.48	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
217.132.138.74	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sip_storage/files/9/	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.246.130.60	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/general/null	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
175.44.17.245	China	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/	None	1
109.67.215.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	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

09-22-2016-23:04:02 to 09-23-2016-00:04:02