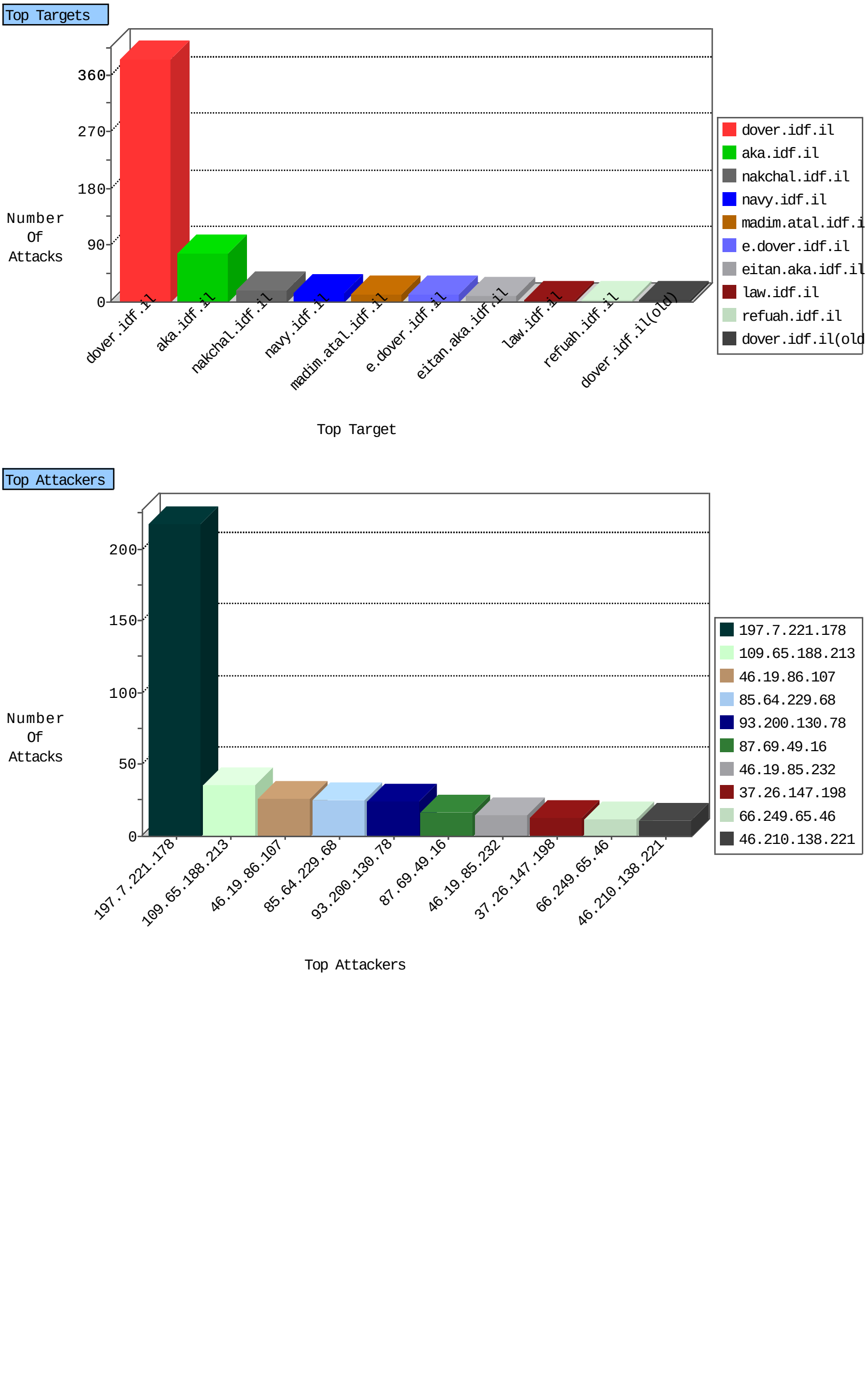
09-18-2016-06:04:07 to 09-18-2016-07:04:07

IDF Under Attack
Daily Report



09-18-2016-06:04:07 to 09-18-2016-07:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.128.107	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	7
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
170.140.119.70	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.133.224.147	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	2
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
123.59.59.52	China	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	1
198.82.160.221	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-18-2016-06:04:07 to 09-18-2016-07:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.202.48.192	France	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.211.2	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
71.6.167.142	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

09-18-2016-06:04:07 to 09-18-2016-07:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
49.248.35.58	147.237.0.34	India	tikshuv.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
212.129.61.237	147.237.0.35	France	akaws.idf.il	ET SCAN Potential SSH Scan	1
109.236.80.12	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential SSH Scan	1
66.249.76.118	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
62.215.38.173	147.237.76.38	Kuwait	e.e.meitav.idf.i	ET SCAN NMAP -sS window 2048	1
50.84.213.146	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 3072	1
50.84.213.146	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -f -sS	1
5.255.90.133	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
212.129.61.237	147.237.77.216	France	dover.idf.il	ET SCAN Potential SSH Scan	1
212.129.61.237	147.237.0.34	France	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
109.236.80.12	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
62.215.38.173	147.237.76.38	Kuwait	e.e.meitav.idf.i	ET SCAN NMAP -sS window 3072	1
62.215.38.173	147.237.76.38	Kuwait	e.e.meitav.idf.i	ET SCAN NMAP -f -sS	1
50.84.213.146	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 2048	1

09-18-2016-06:04:07 to 09-18-2016-07:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	210
109.65.188.213	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
85.64.229.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
93.200.130.78	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
87.69.49.16	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
37.26.147.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
66.249.65.46	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.210.138.221	Israel	147.237.77.212	e.dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
31.168.79.117	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.107	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.86.107	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
185.3.147.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
91.135.102.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.65.188.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
91.135.102.191	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
197.7.221.178	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
109.65.188.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.65.188.213	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.65.10.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
109.65.188.213	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
85.250.214.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.26.147.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	2
213.57.135.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.147.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
46.19.85.223	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
139.162.37.147	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
2.55.181.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
198.223.242.46	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.13.231.122	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
37.26.147.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
114.98.244.254	China	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
185.112.188.72	Iraq	147.237.76.177	ncore.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
184.105.139.76	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
120.132.67.190	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
70.211.159.95	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.21	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.139	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.211	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.0.33	idf.il	drop		drop	1

09-18-2016-06:04:07 to 09-18-2016-07:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.56.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
185.3.147.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
217.132.51.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.76.118	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
40.77.167.73	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
66.249.79.139	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1302-he/refuah.aspx	Block	1
66.249.66.103	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
68.180.229.223	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	1
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
87.68.27.224	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
176.13.4.173	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$emailUpdate$rptEmailSubjectsList$ctl00$cbEmailSubject in www.aka.idf.il/main/giyus/faq.aspx	None	1
5.29.139.26	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1

09-18-2016-06:04:07 to 09-18-2016-07:04:07