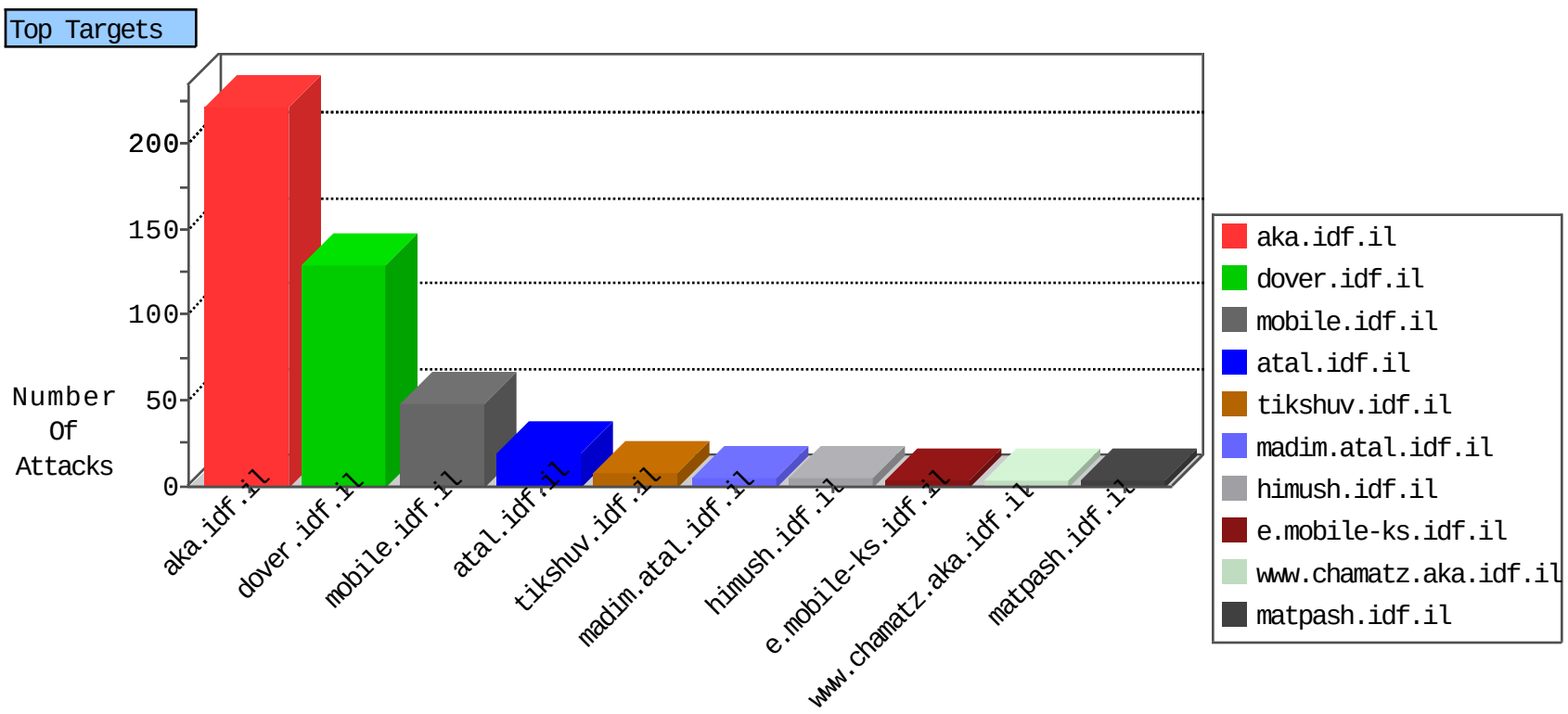
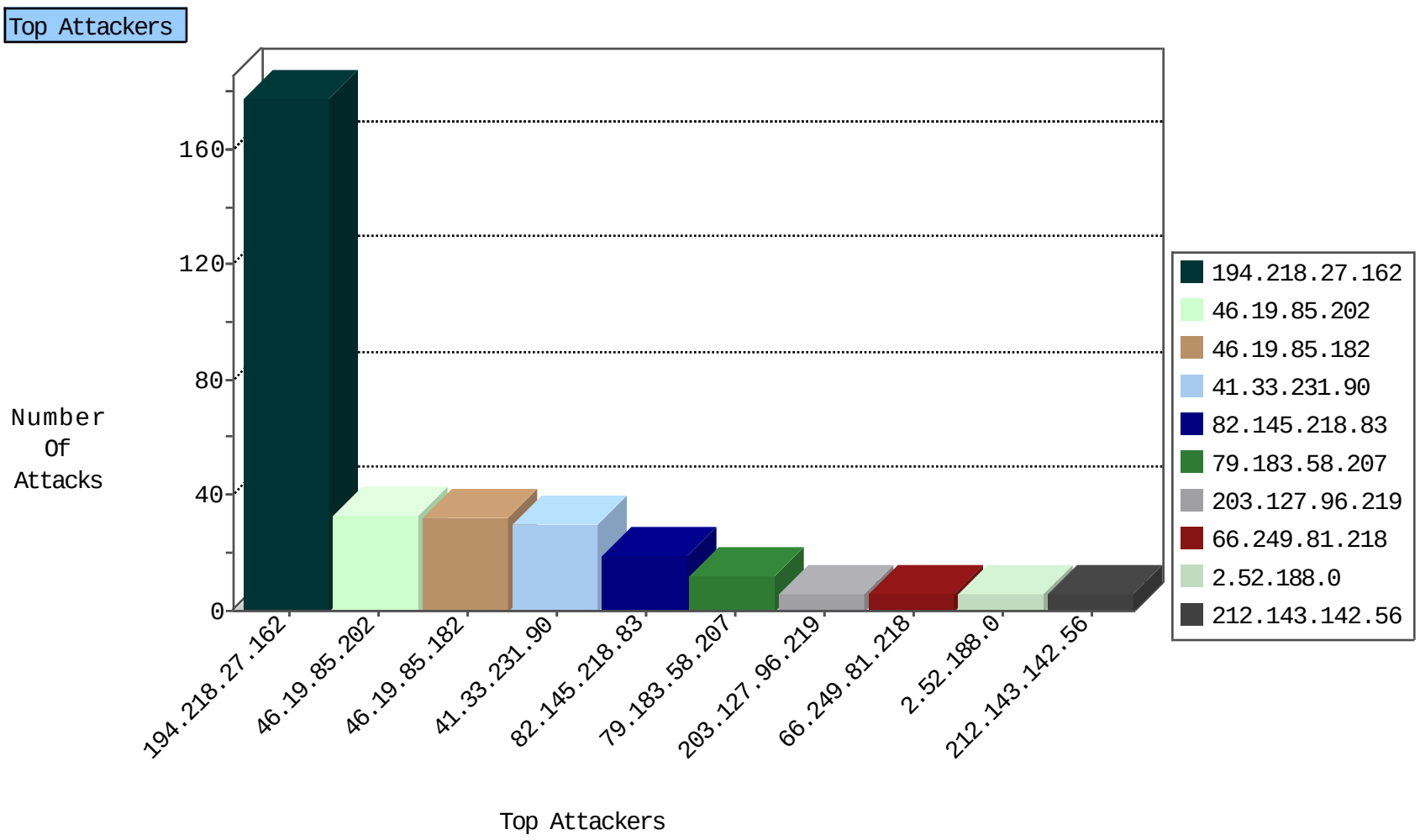
03-01-2016-01:12:14 to 03-01-2016-02:12:14

IDF Under Attack Daily Report





03-01-2016-01:12:14 to 03-01-2016-02:12:14

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.218.83	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	19
217.26.171.188	Moldova, Republic of	147.237.77.176	matpash.idf.il	L4 Source or Dest Port Zero	drop	2
185.130.5.201		147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.246		147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
58.56.44.229	China	147.237.77.235	sviva.idf.il	JLM_Purple_Con_Limit_Http	drop	1
185.130.5.224		147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
192.3.27.250	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.246		147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
217.26.171.188	Moldova, Republic of	147.237.76.176	test.ncore.idf.il	L4 Source or Dest Port Zero	drop	1
183.254.128.111	China	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.246		147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

03-01-2016-01:12:14 to 03-01-2016-02:12:14

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.110	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
173.234.159.250	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
199.30.24.212	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
93.219.97.171	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
40.77.167.88	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
162.250.190.142	Canada	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1

03-01-2016-01:12:14 to 03-01-2016-02:12:14

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
104.192.0.19	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.224.162.108	147.237.76.34	Hungary	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.244.49.137	147.237.0.34	Hong Kong	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.0.35	Latvia	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.0.17	Latvia	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
120.72.118.152	147.237.76.200	Vietnam	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
104.192.0.20	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.192.0.19	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.255.21.58	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1
63.221.141.195	147.237.0.200	Hong Kong	m4u.idf.il	ET SCAN Potential SSH Scan	1
61.244.49.137	147.237.0.33	Hong Kong	idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.0.33	Latvia	idf.il	ET SCAN NMAP -sS window 1024	1
120.72.118.152	147.237.76.200	Vietnam	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.192.0.19	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

03-01-2016-01:12:14 to 03-01-2016-02:12:14

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	118
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.85.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
46.19.85.202	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
46.19.85.202	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.183.58.207	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.188.0	Israel	147.237.72.166	aka.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	6
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.22.131.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.250.16.72	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.187	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.102.195.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.14.86	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.179.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.20.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.129.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.167.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.162.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.130.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.19.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
63.171.19.251	Yemen	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.121.122.48	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
203.127.96.219	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.46.39.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
203.127.96.219	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
203.127.96.219	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
63.171.19.251	Yemen	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
213.233.85.159	Romania	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
113.76.90.199	China	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
80.82.79.104	Netherlands	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
203.127.96.221	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
106.38.241.106	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
69.112.97.39	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.145	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.244.75.181	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
203.127.96.221	Singapore	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
40.118.170.50	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.146	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

03-01-2016-01:12:14 to 03-01-2016-02:12:14

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.244.75.181	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.22.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP anomaly detected	Non-compliant TCP packets coming from multiple external sources were detected. This may result from potential network configuration problem.	drop	1
40.118.170.50	United States	147.237.0.33	idf.il	drop		drop	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
113.76.90.199	China	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
80.82.79.104	Netherlands	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.121.122.48	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

03-01-2016-01:12:14 to 03-01-2016-02:12:14

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.81.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
46.19.85.182	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
79.183.58.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.109.245.36	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 87.109.245.36	Block	3
208.113.248.206	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 208.113.248.206	Block	3
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.66.184	Block	2
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	2
70.194.71.12	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.9.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.81.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
208.115.113.89	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/kishur/default.asp	Block	1
66.249.66.179	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/pazan_in_pictures/kkkkkkk=7f4d68a4kkkkkkk_7f4d68a4	Block	1
1.4.175.242	Thailand	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
220.255.103.5	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/main/giyus/general.aspx	Block	1
203.127.96.201	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
24.61.14.98	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.109.245.36	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
95.86.82.230	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
208.113.248.206	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
59.100.228.98	Australia	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1

03-01-2016-01:12:14 to 03-01-2016-02:12:14