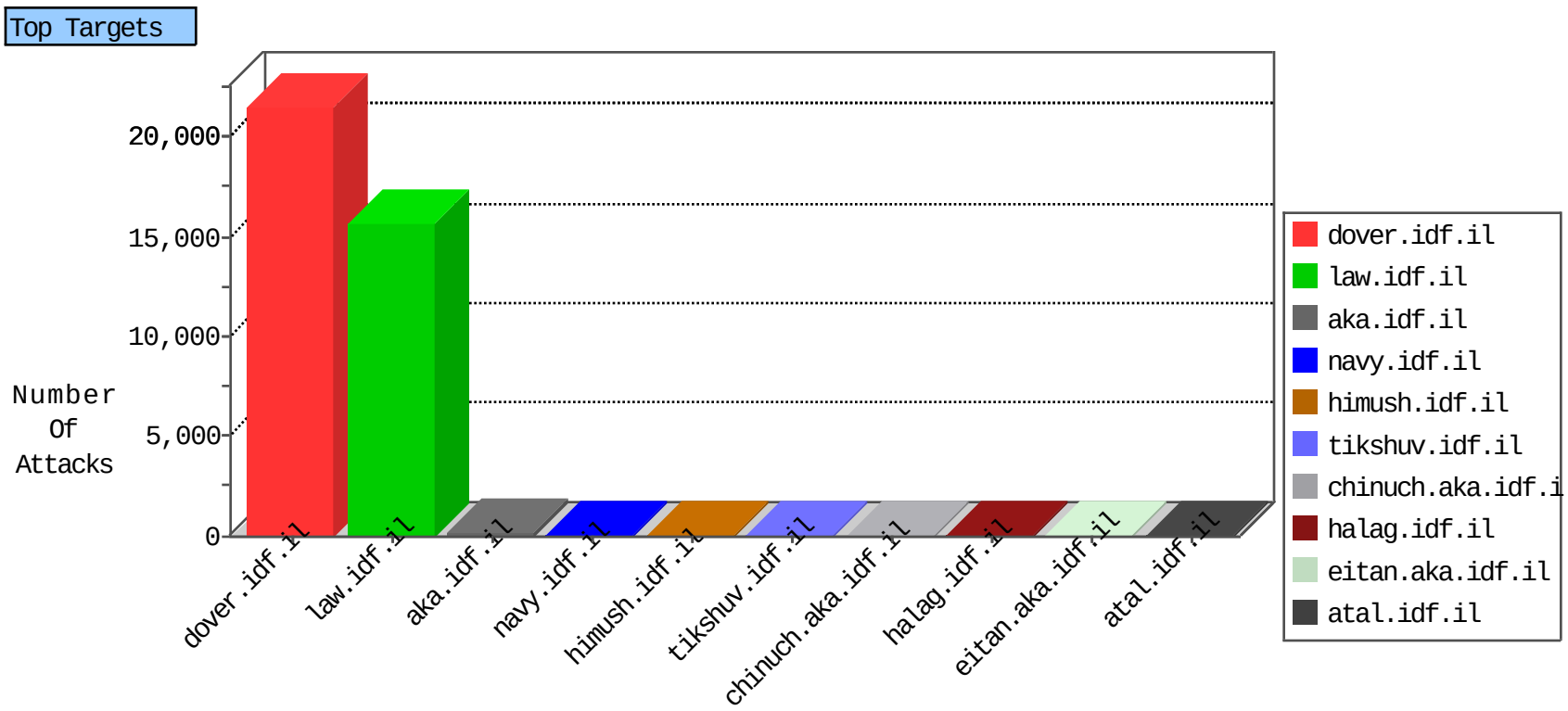
04-23-2016-06:04:02 to 04-23-2016-07:04:02

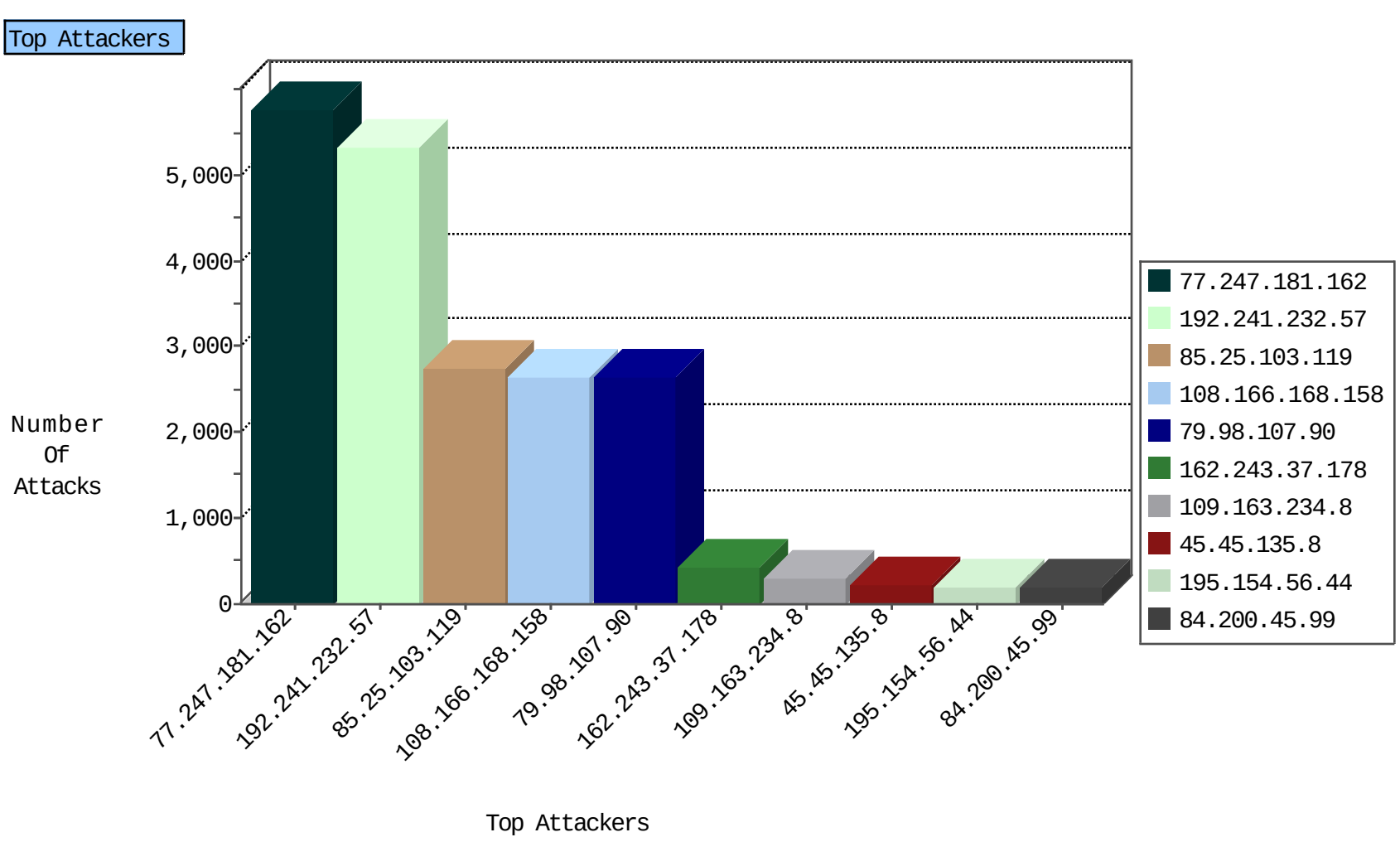
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-23-2016-06:04:02 to 04-23-2016-07:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.241.232.57	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7025
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4083
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3871
77.247.181.163	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3845
5.157.57.78	Sweden	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3138
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3057
197.115.63.32	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2749
45.45.135.14	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	999
192.241.232.57	United States	147.237.77.216	dover.idf.il	DOS-WEB-HULK-improved	forward	271
91.108.88.169	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	255
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	DOS-HTTP-torshammer	dest-reset	15
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	10
192.241.232.57	United States	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	6
91.108.88.219	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2
79.98.107.90	Bulgaria	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
65.19.167.131	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
84.200.45.99	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2
45.45.135.8	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2
91.108.88.83	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
45.45.135.20	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
185.103.252.98	Russian Federation	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
45.45.135.9	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
5.157.57.45	Sweden	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
185.103.252.98	Russian Federation	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
109.163.234.8	Romania	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	1
45.45.135.12	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
91.108.88.180	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
89.46.102.242	Romania	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
183.60.48.25	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
91.108.88.196	Germany	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1

04-23-2016-06:04:02 to 04-23-2016-07:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.241.232.57	United States	147.237.77.216	dover.idf.il	12371: TCP: Hulk DDoS Tool	Block	9

04-23-2016-06:04:02 to 04-23-2016-07:04:02

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
174.37.194.144	147.237.76.30	United States	himush.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.17	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
174.37.194.144	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 2048	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.38	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.78.158	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
13.92.122.143	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
188.138.25.228	147.237.0.19	France	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.99	147.237.8.28	Lithuania	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 4096	1
174.37.194.144	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -f -sS	1
91.106.93.21	147.237.77.234	Iran, Islamic Republic of	halag.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
40.114.42.13	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
188.138.25.228	147.237.0.19	France	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
1.34.89.177	147.237.0.19	Taiwan	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
187.160.213.25	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

04-23-2016-06:04:02 to 04-23-2016-07:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5772
192.241.232.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5249
85.25.103.119	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2738
79.98.107.90	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2638
108.166.168.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2601
162.243.37.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	429
109.163.234.8	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	290
45.45.135.8	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	225
195.154.56.44	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	197
84.200.45.99	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	194
5.157.57.78	Sweden	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	188
91.108.88.95	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	184
84.200.45.226	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	182
45.45.135.19	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	178
23.81.248.8	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	164
45.45.135.17	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	156
23.106.166.163	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	153
23.106.161.77	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	152
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	150
91.108.88.94	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	144
23.81.235.107	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	143
5.157.57.2	Sweden	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	142
5.157.57.82	Sweden	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	142
5.157.57.9	Sweden	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	141
84.200.45.91	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	138
8.18.121.17	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	138
23.81.69.221	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	137
45.45.135.12	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	136
91.108.88.143	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	136
23.106.244.77	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	133
91.108.88.249	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	123
91.108.88.238	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	122
23.106.161.126	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	121
91.108.88.231	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	121
38.111.147.84	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	120
104.251.82.125	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	117
192.241.189.66	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	117
8.18.120.97	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	114
91.108.88.3	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	113
23.81.205.124	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	108
8.18.121.238	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	106
23.106.205.104	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	104
104.251.90.22	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	103
8.18.121.246	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	103
91.108.88.120	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	101
91.108.88.73	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	100
23.81.247.85	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	100
91.108.88.243	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	99
8.18.120.105	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	99
5.157.57.14	Sweden	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	98

04-23-2016-06:04:02 to 04-23-2016-07:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.147.190.205	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
174.37.194.144	United States	147.237.76.30	himush.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/links.aspx	Block	1
141.212.122.161	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/	Block	1
62.210.170.165	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/cgi-bin/shitur/bookpage100598/iturfindpageexact.pl	Block	1
184.105.139.68	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
216.218.206.67	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.39.191	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/contactus.aspx	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
199.30.24.117	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.183.164.80	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
157.55.39.250	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.65.80	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.115.111.73	Block	1
87.71.43.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
174.37.194.144	United States	147.237.76.30	himush.idf.il	Multiple Untraceable SSL Sessions from 174.37.194.144 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 208.115.113.82	Block	1
89.248.160.136	Netherlands	147.237.76.30	himush.idf.il	Illegal HTTP Version	Block	1

04-23-2016-06:04:02 to 04-23-2016-07:04:02