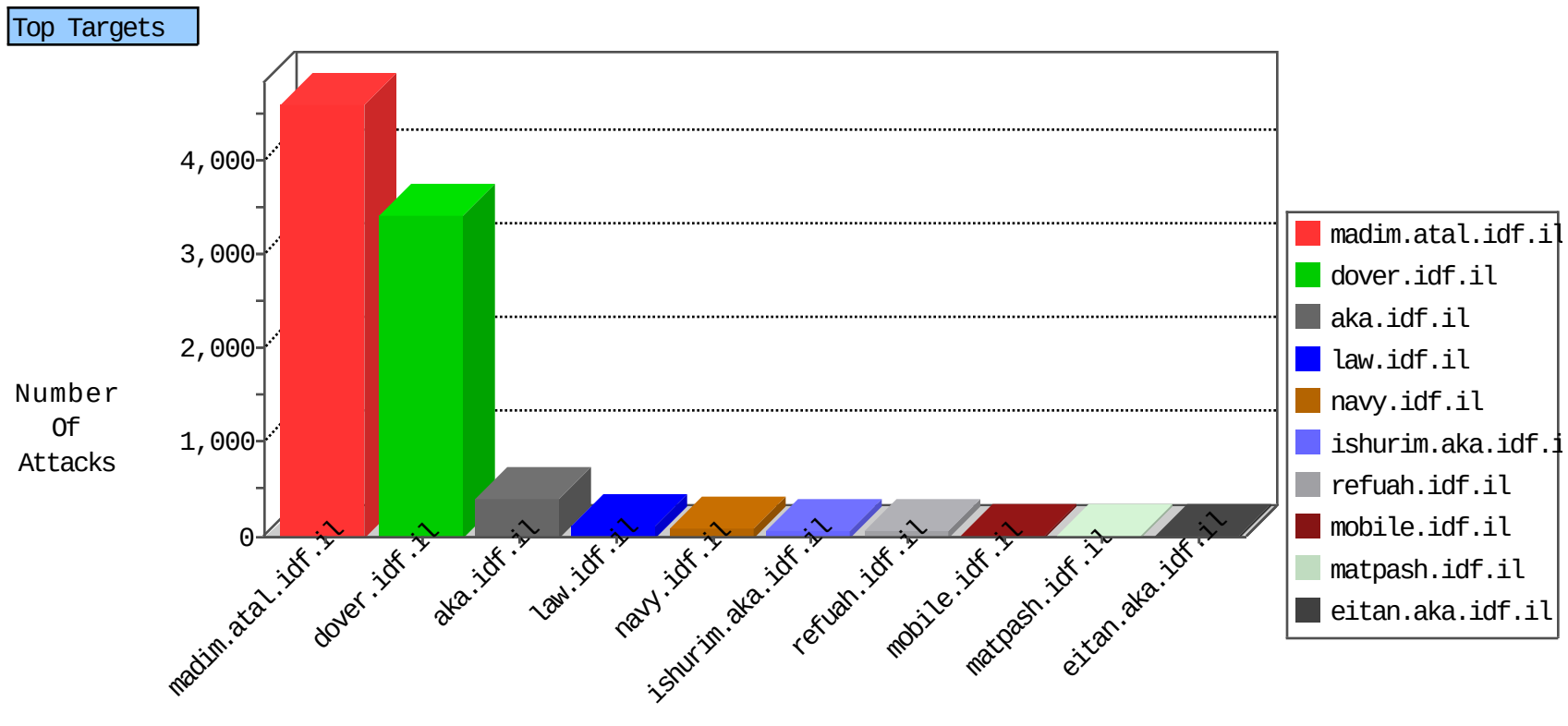
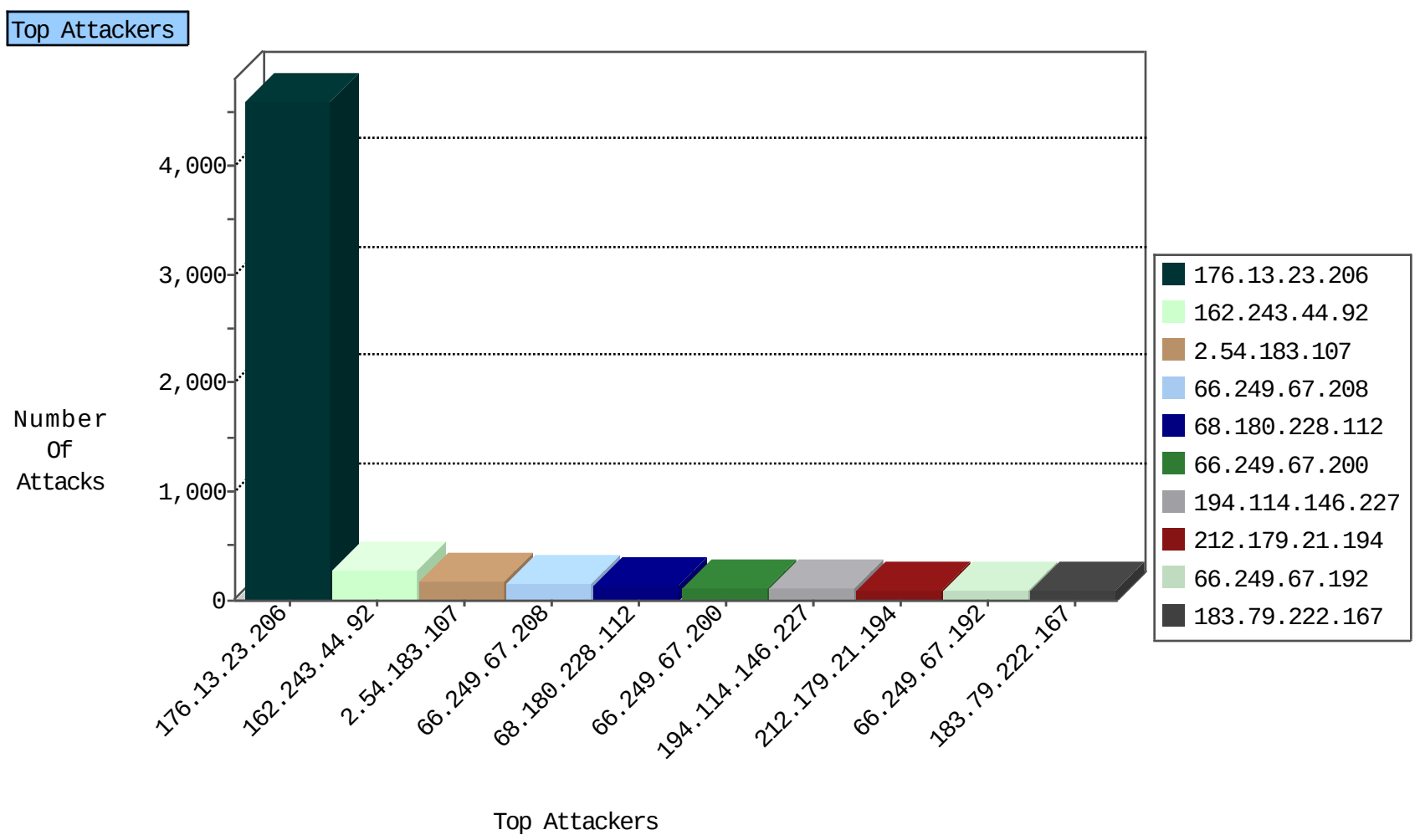
10-21-2015-08:04:04 to 10-21-2015-09:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-21-2015-08:04:04 to 10-21-2015-09:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.148.96	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	68
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	51
84.108.69.24	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
81.218.50.34	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
81.218.46.131	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	29
46.19.85.171	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
2.54.3.171	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	17
2.54.3.171	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
124.83.37.157	Philippines	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
81.218.234.122	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
2.54.59.140	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
176.12.148.96	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
46.19.85.191	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
212.179.166.210	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
82.80.196.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
91.228.127.198	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
212.143.144.237	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
46.19.86.222	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
192.116.98.164	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
176.12.149.134	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
199.203.215.1	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.15.56	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
84.108.13.14	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.19.86.53	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
82.80.26.75	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.132.59.216	Kazakstan	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
84.228.191.16	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
149.88.228.88	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.176.106.217	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.12.145.149	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.181.201.14	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.63.173	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
79.181.201.14	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.37.2	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
115.231.222.40	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Http	drop	2
81.218.234.122	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
2.54.171.5	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.86.53	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.63.173	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
176.12.141.77	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
81.218.29.162	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
176.12.148.238	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
2.52.47.32	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-21-2015-08:04:04 to 10-21-2015-09:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-21-2015-08:04:04 to 10-21-2015-09:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
218.200.188.213	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
217.194.199.124	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.100.85.71	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
101.1.17.53	147.237.0.34	Hong Kong	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
80.179.114.19	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.200.188.213	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
218.200.188.213	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
192.161.63.49	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
174.128.228.82	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.67.208	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
45.33.70.65	147.237.77.205		prisha.idf.il	ET SCAN Potential SSH Scan	1
31.44.66.72	147.237.76.39	Albania	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-21-2015-08:04:04 to 10-21-2015-09:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
162.243.44.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	249
2.54.183.107	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	181
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	93
46.19.86.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	88
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
80.178.212.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
103.7.197.12	Vanuatu	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
192.200.155.168	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
176.12.148.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
37.26.149.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
124.83.37.157	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
2.54.3.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
79.181.3.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
81.218.46.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
79.176.126.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
183.79.222.167	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
80.74.116.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
66.249.67.200	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
37.26.149.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
81.218.234.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.249.67.208	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
2.54.4.222	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	21
46.117.96.55	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
46.19.85.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
46.19.86.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
176.12.148.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
100.100.30.216		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
192.114.91.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.86.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
176.13.19.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	17
194.114.146.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
79.178.59.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
81.218.251.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
81.218.50.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
141.0.13.75	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
212.143.144.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
2.52.22.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
192.117.148.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.23.206	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.23.206	Block	4576
66.249.67.208	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.208	Block	104
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	104
194.114.146.227	Israel	147.237.77.74	law.idf.il	Suspicious Response Code	Block	78
66.249.67.200	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.200	Block	78
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	52
183.79.222.167	Japan	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	52
66.249.67.192	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.192	Block	39
66.249.67.192	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	26
37.26.149.252	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	26
79.176.126.226	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	26
2.54.32.106	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	26
212.179.102.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	26
77.237.138.51	Czech Republic	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	13
216.218.206.68	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	13
2.54.2.98	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	13
183.79.222.167	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jenin.stm" target="_blank	Block	13
109.160.135.67	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
202.102.99.107	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/webresource.axd%3fd	Block	13
184.105.247.196	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	13
146.185.234.48	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/links/links.aspx/templates/sendtofriend/sendtofriend.aspx	Block	13
207.232.5.66	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	13
66.249.67.135	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/kapatz/default.aspx	Block	13
180.153.180.76	China	147.237.77.176	matpash.idf.il	URL is Above Root Directory www.cogat.idf.il/../shared/clientscripts/sidebar/sidebar.js	Block	13
79.177.197.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
66.249.67.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	13
2.54.171.151	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22824-he/dover.as	Block	13
162.243.44.92	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 162.243.44.92	Block	13
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9709-he/refuah.aspx	Block	13
208.115.111.73	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
66.249.67.178	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	13
182.118.60.140	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/shared/clientscripts/imagevideogallerylobby/imagevideogallerylobby.js%3fsiteversion	Block	13
80.246.136.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/4/size220x0/17404.jpg	Block	13
37.26.146.191	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
176.13.15.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	13
66.249.67.192	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
84.95.251.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
66.249.67.208	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
199.16.156.126	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/4/size220x0/17404.jpg	Block	13
37.26.149.252	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	13
176.13.23.206	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	13

10-21-2015-08:04:04 to 10-21-2015-09:04:04