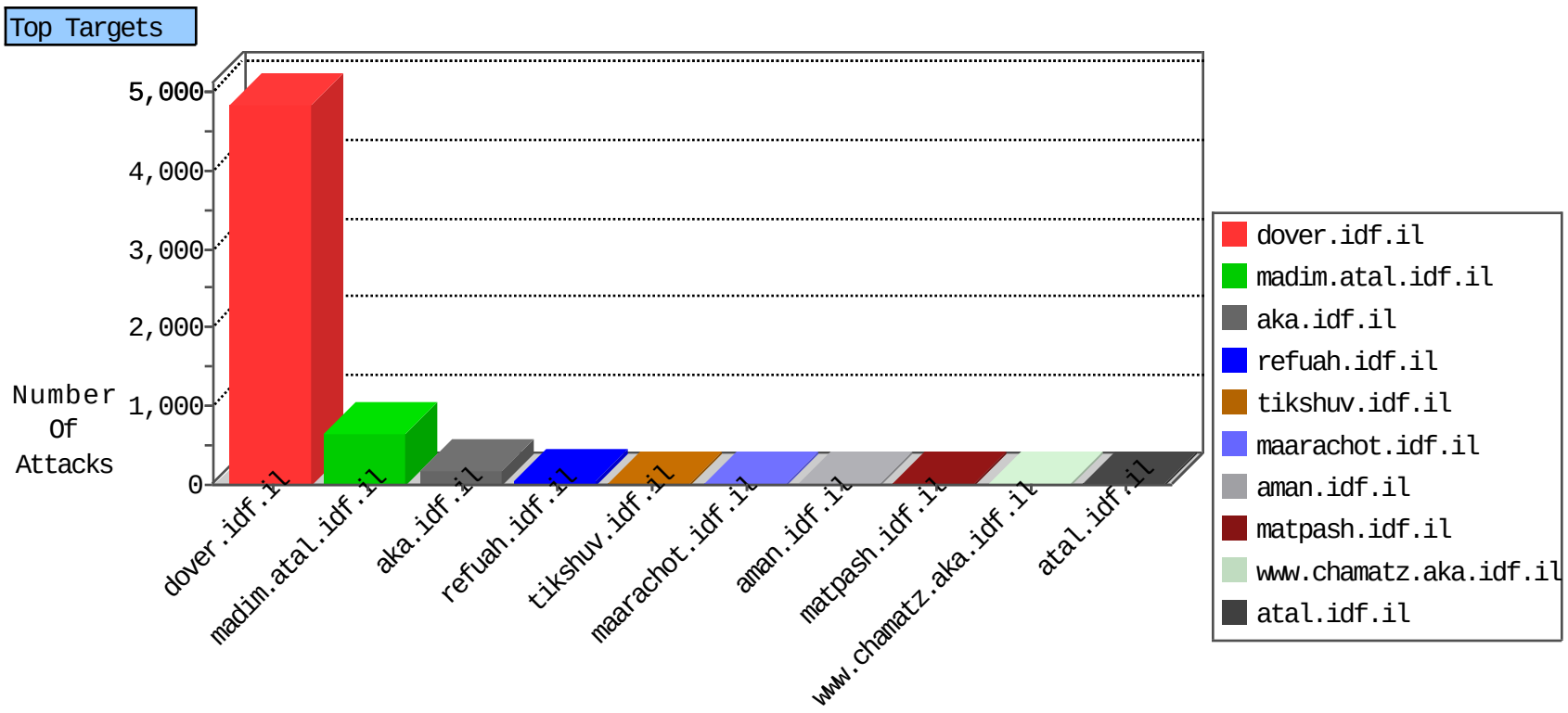
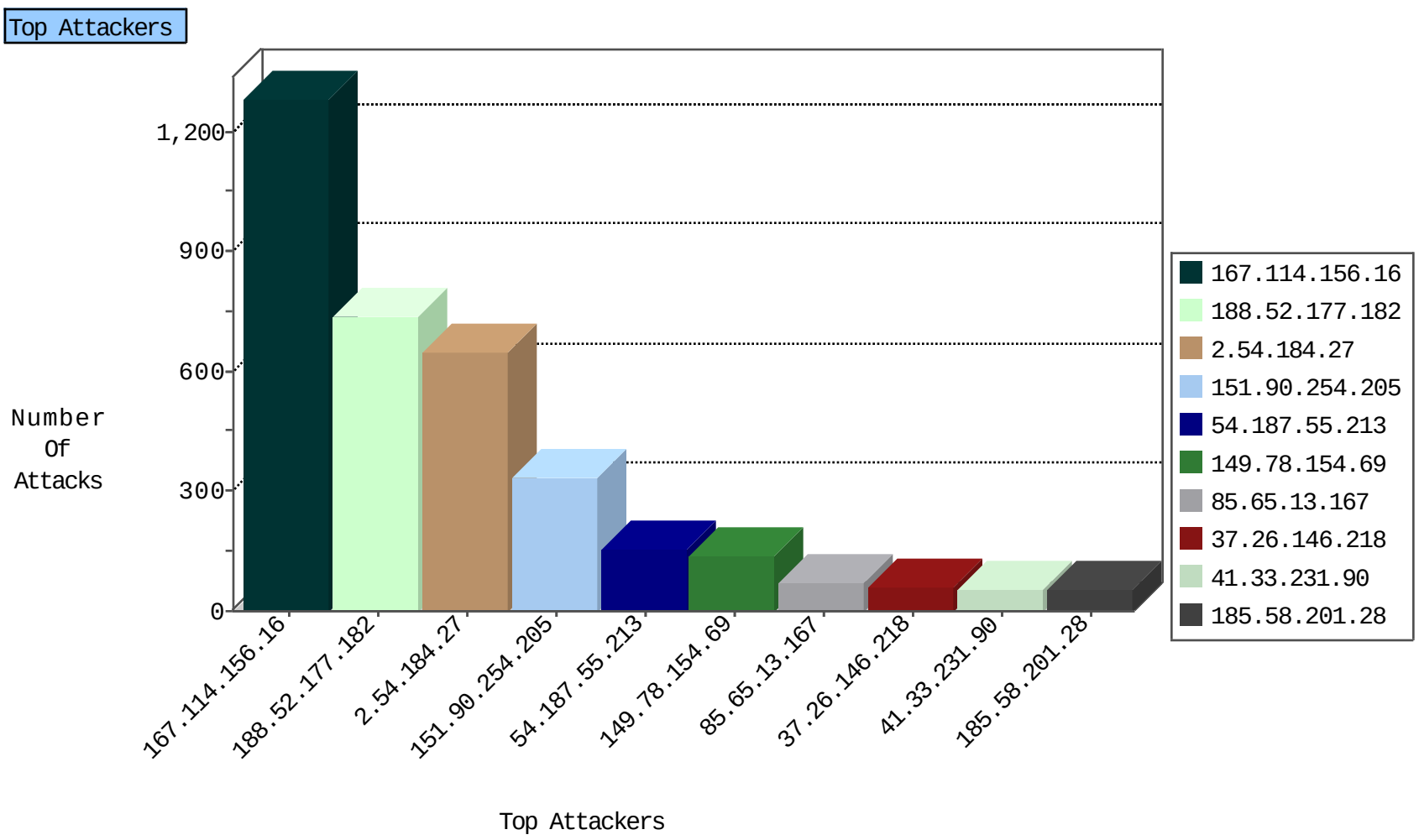
11-06-2015-18:04:00 to 11-06-2015-19:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-06-2015-18:04:00 to 11-06-2015-19:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.216	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3161
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2437
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	551
83.149.99.157	Netherlands	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	7
83.149.99.157	Netherlands	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	7
109.67.2.168	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.176.166.206	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.181.171.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
93.184.6.2	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
66.249.65.238	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
38.108.216.178	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
213.149.223.82	Italy	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.117.75.244	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
37.8.115.39	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
178.81.24.99	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.i	Block_Udp_All_Nets	drop	3
188.53.160.212	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
83.149.99.157	Netherlands	147.237.76.201	e.atal.idf.il	Invalid TCP Flags	drop	2
109.65.117.60	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
2.54.47.225	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.8.115.39	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

11-06-2015-18:04:00 to 11-06-2015-19:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-06-2015-18:04:00 to 11-06-2015-19:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
188.52.177.182	147.237.77.216	Saudi Arabia	dover.idf.il	SQL generic sql with comments injection attempt - GET parameter	19
188.52.177.182	147.237.77.216	Saudi Arabia	dover.idf.il	SQL Injection - Select From	16
188.52.177.182	147.237.77.216	Saudi Arabia	dover.idf.il	INDICATOR-OBFUSCATION large number of calls to char function - possible sql injection obfuscation	12
188.52.177.182	147.237.77.216	Saudi Arabia	dover.idf.il	XSS - IMG (POST)	10
188.52.177.182	147.237.77.216	Saudi Arabia	dover.idf.il	ET WEB_SERVER MYSQL SELECT CONCAT SQL Injection Attempt	10
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	9
188.52.177.182	147.237.77.216	Saudi Arabia	dover.idf.il	ET WEB_SERVER Possible MySQL SQLi Attempt Information Schema Access	9
188.52.177.182	147.237.77.216	Saudi Arabia	dover.idf.il	SERVER-WEBAPP encoded cross site scripting HTML Image tag attempt	6
188.52.177.182	147.237.77.216	Saudi Arabia	dover.idf.il	SQL use of concat function with select - likely SQL injection	5
188.52.177.182	147.237.77.216	Saudi Arabia	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
188.52.177.182	147.237.77.216	Saudi Arabia	dover.idf.il	SQL Injection - Select From (POST)	4
66.249.81.145	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.158	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
94.23.49.49	147.237.77.170	France	maarachot.idf.il	SERVER-WEBAPP backup access	2
221.179.89.90	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
83.149.99.157	147.237.72.166	Netherlands	aka.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.159	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
79.176.150.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.151.52.8	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -sS window 1024	1
113.121.170.46	147.237.77.212	China	e.dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
222.190.111.119	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
83.149.99.157	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	1
221.179.89.90	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
83.149.99.157	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1
66.249.65.238	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
46.151.52.8	147.237.72.166	Ukraine	aka.idf.il	ET SCAN NMAP -sS window 1024	1
27.185.104.53	147.237.77.205	China	prisha.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

11-06-2015-18:04:00 to 11-06-2015-19:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.52.177.182	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	628
151.90.254.205	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	335
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	152
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	139
85.65.13.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
37.26.146.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
185.58.201.28	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
149.78.170.87	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
198.17.111.194	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
2.54.30.49	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
2.52.188.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
82.192.68.46	Netherlands	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
100.100.92.167		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	31
131.91.4.36	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
84.228.120.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
46.19.85.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
37.142.64.41	Israel	147.237.76.42	refuah.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
63.143.229.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
66.249.88.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
78.95.98.179	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
207.46.13.68	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
189.123.219.116	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.116.71.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
100.100.14.43		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
2.54.145.17	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
98.116.92.50	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
93.173.249.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.66.182.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
149.200.238.152	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
100.100.124.143		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
92.241.53.173	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
37.237.232.130	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
87.69.220.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
114.108.229.196	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13

11-06-2015-18:04:00 to 11-06-2015-19:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.184.27	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.184.27	Block	370
2.54.184.27	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.184.27	Block	172
2.54.184.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
5.29.78.154	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	10
94.23.49.49	France	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	8
94.23.49.49	France	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 94.23.49.49	Block	7
87.69.62.227	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.62.227	Block	4
50.63.138.151	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 50.63.138.151	Block	4
37.26.148.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.94.188.30	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
89.138.251.35	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	2
66.249.79.25	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
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	2
176.12.142.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.154.92.165	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	2
109.64.108.28	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
62.210.88.201	France	147.237.77.234	halag.idf.il	Unauthorized URL Access to 51.254.206.142/httptest.php	Block	1
31.154.92.165	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 31.154.92.165	Block	1
87.69.33.182	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
66.249.67.224	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/×″×?×ª×¨	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
139.193.9.80	Indonesia	147.237.77.74	law.idf.il	Illegal Byte Code Character in Header Value	Block	1
94.23.49.49	France	147.237.77.170	maarachot.idf.il	Multiple Admin Blocking from 94.23.49.49	Block	1
46.117.247.97	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
182.118.55.217	China	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
66.249.67.102	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.67.102	Block	1
109.64.141.162	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz/resources/images/innerpage/goback.gif	Block	1
65.49.68.157	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
31.154.92.165	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/3/	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
139.193.9.80	Indonesia	147.237.77.74	law.idf.il	Multiple Illegal Byte Code Character in Header Value from 139.193.9.80	Block	1
182.118.60.53	China	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/	Block	1
66.249.67.102	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/modules/forums.frm/frmprintmessage.aspx	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1628-he/refuah.aspx	Block	1
109.65.189.231	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.69.62.227	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
66.249.79.28	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.29	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/	Block	1
58.180.228.110	Korea, Republic of	147.237.77.176	matpash.idf.il	URL is Above Root Directory www.cogat.idf.il/../shared/usercontrols/headerupper/	Block	1
79.180.57.139	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.52.177.182	Saudi Arabia	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.122	Block	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/size100x0/3126.jpg	Block	1
109.65.209.251	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
37.142.64.41	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
87.69.220.99	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1246-he/atal.aspx	Block	1
66.249.79.31	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1

11-06-2015-18:04:00 to 11-06-2015-19:04:00