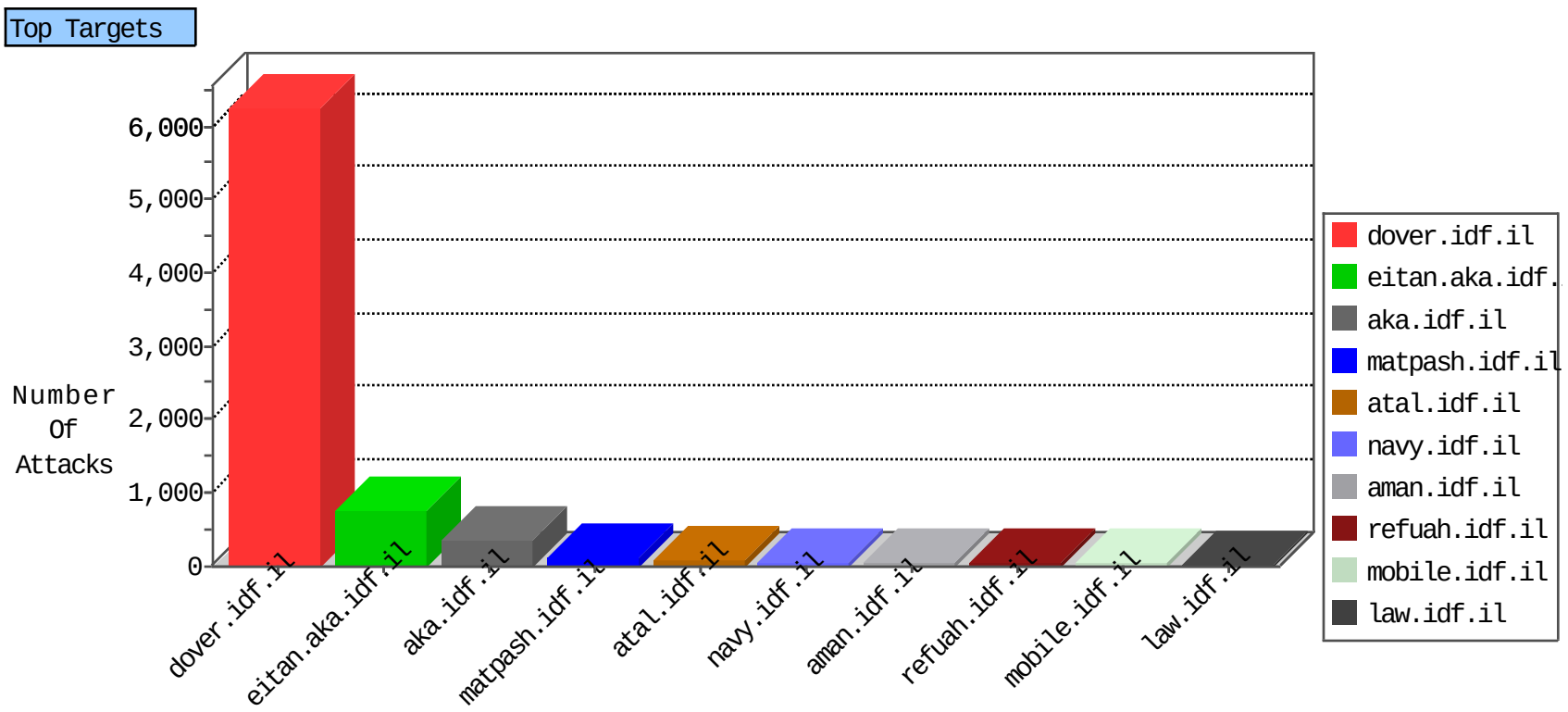
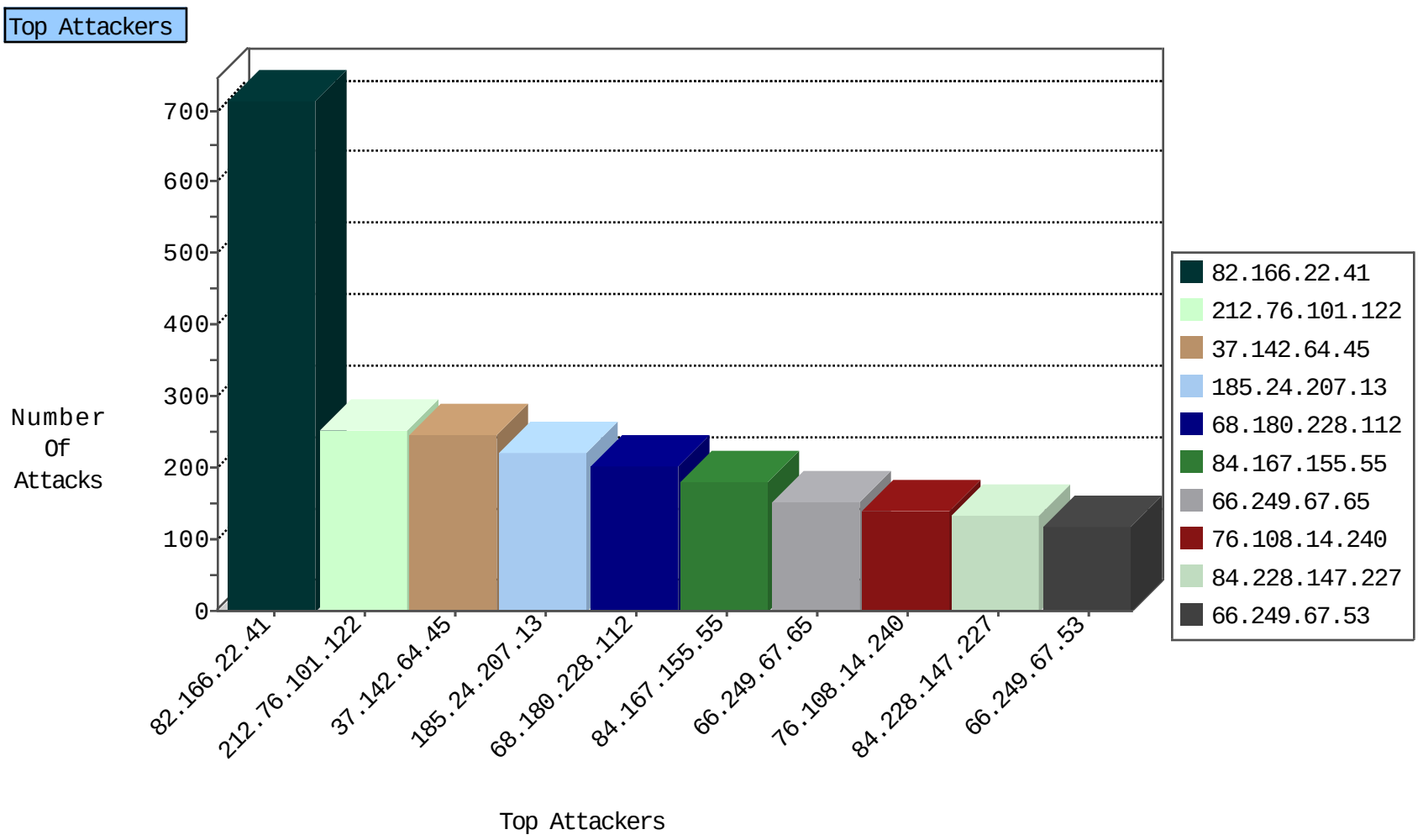
10-24-2015-23:04:06 to 10-25-2015-00:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-24-2015-23:04:06 to 10-25-2015-00:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	158
84.236.37.40	Hungary	147.237.77.216	dover.idf.il	SYN Flood full table	drop	17
185.32.179.187	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
177.82.158.64	Brazil	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
109.66.81.104	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
149.78.226.237	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.64.17.180	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
2.54.179.103	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
85.115.52.201	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.66.81.104	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
10.0.0.3		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
73.46.229.171	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
5.29.231.34	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
95.71.120.223	Russian Federation	147.237.72.167	ishurim.aka.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
79.181.57.154	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.120.41.204	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
176.12.147.91	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-24-2015-23:04:06 to 10-25-2015-00:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-24-2015-23:04:06 to 10-25-2015-00:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.124	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	18
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
81.88.116.80	147.237.72.217	Russian Federation	e.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.151.52.8	147.237.0.15	Ukraine	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
195.20.154.142	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
122.180.230.142	147.237.76.30	India	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
103.232.35.93	147.237.8.50	Hong Kong	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
93.174.89.142	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
67.176.133.24	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
195.20.154.142	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
195.20.154.142	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
104.43.200.179	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.8.27	Netherlands	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	1

10-24-2015-23:04:06 to 10-25-2015-00:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
82.166.22.41	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	387
212.76.101.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	252
37.142.64.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	245
185.24.207.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	221
84.167.155.55	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	182
76.108.14.240	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	140
84.228.147.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	135
71.234.239.61	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	117
89.139.168.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	104
89.108.144.114	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	92
2.54.144.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
109.186.61.100	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	80
68.180.230.29	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	76
66.87.125.234	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
37.210.175.20	Qatar	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
85.65.127.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
46.19.86.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
46.19.86.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
109.66.209.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
79.176.15.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
80.179.22.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
176.13.9.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
24.234.212.186	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
66.249.67.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
41.227.239.190	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
176.67.122.11	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
79.178.13.94	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
37.26.149.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
89.13.1.19	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
213.151.40.43	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
197.133.255.195	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
66.249.67.65	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
109.65.74.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
86.161.3.59	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
5.29.208.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
99.238.64.246	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30

10-24-2015-23:04:06 to 10-25-2015-00:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.166.22.41	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 82.166.22.41	Block	307
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	56
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	56
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	56
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	42
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	42
199.16.156.126	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.16.156.126	Block	28
41.227.239.190	Tunisia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin	Block	28
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	28
132.66.10.149	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
91.200.12.11	Ukraine	147.237.77.233	atal.idf.il	PHP Attempt	Block	24
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/size220x0/16340.jpg	Block	14
41.227.239.190	Tunisia	147.237.77.216	dover.idf.il	Admin Blocking	Block	14
149.88.109.179	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
82.81.3.242	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx	None	14
66.249.69.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
185.32.179.232	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
46.120.209.42	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	14
91.200.12.11	Ukraine	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 91.200.12.11	Block	14
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	14
41.227.239.190	Tunisia	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 41.227.239.190	Block	14
149.88.109.179	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	14
82.166.22.41	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	14
66.249.78.58	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	14
188.143.232.40	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx	Block	14
66.249.65.181	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
212.76.105.77	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	14
66.249.67.67	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	14
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/12	Block	14
188.165.15.162	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8967-he/refuah.aspx	Block	14
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
91.200.12.11	Ukraine	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/xmlrpc.php	Block	14
77.125.9.8	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
66.249.67.77	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	14
212.76.105.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
46.116.72.181	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
182.118.21.246	China	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
87.69.200.236	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	14
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/17348.jpg	Block	14
5.79.74.89	Netherlands	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	14
80.246.136.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
66.249.67.190	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	14
46.120.41.204	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	14
183.79.219.111	Japan	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
89.139.16.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	14
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	14

10-24-2015-23:04:06 to 10-25-2015-00:04:06