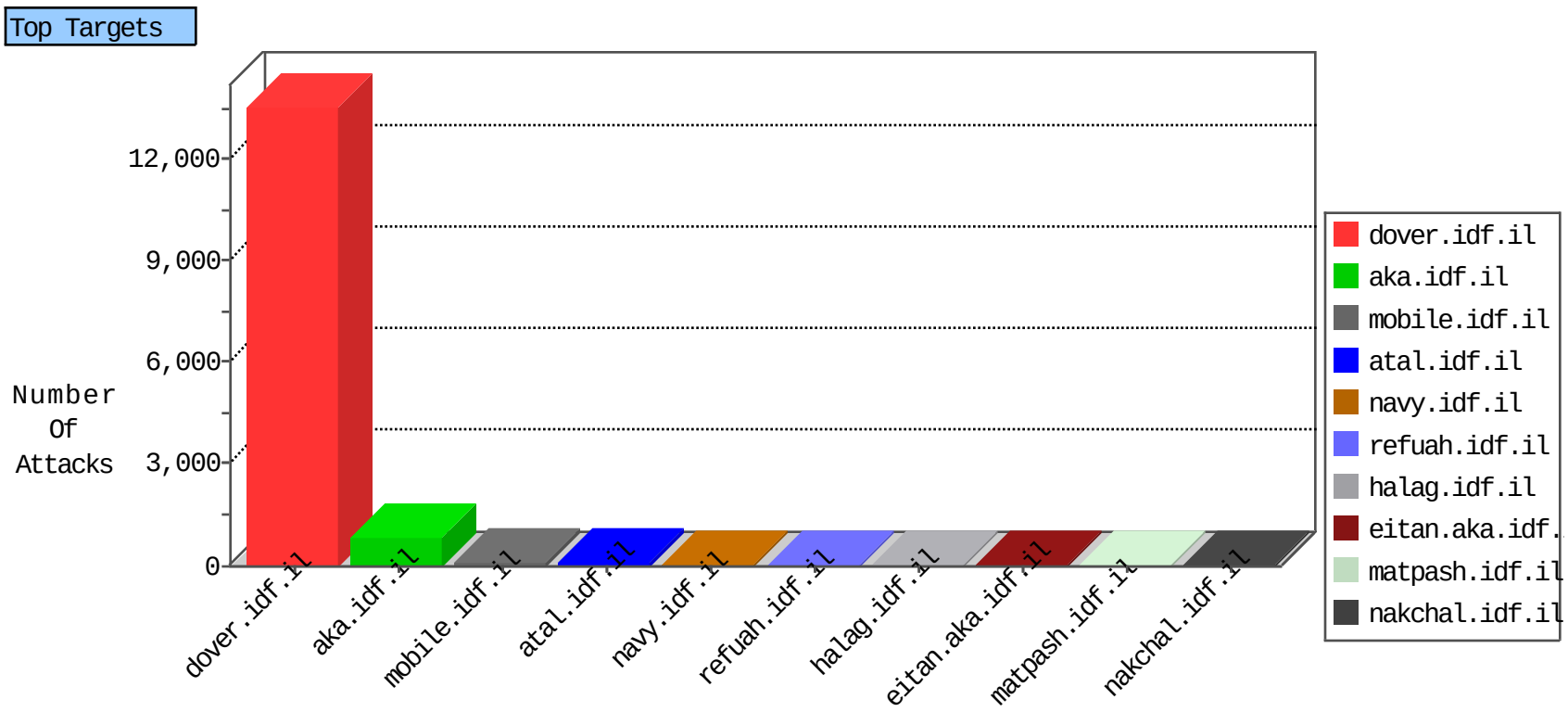
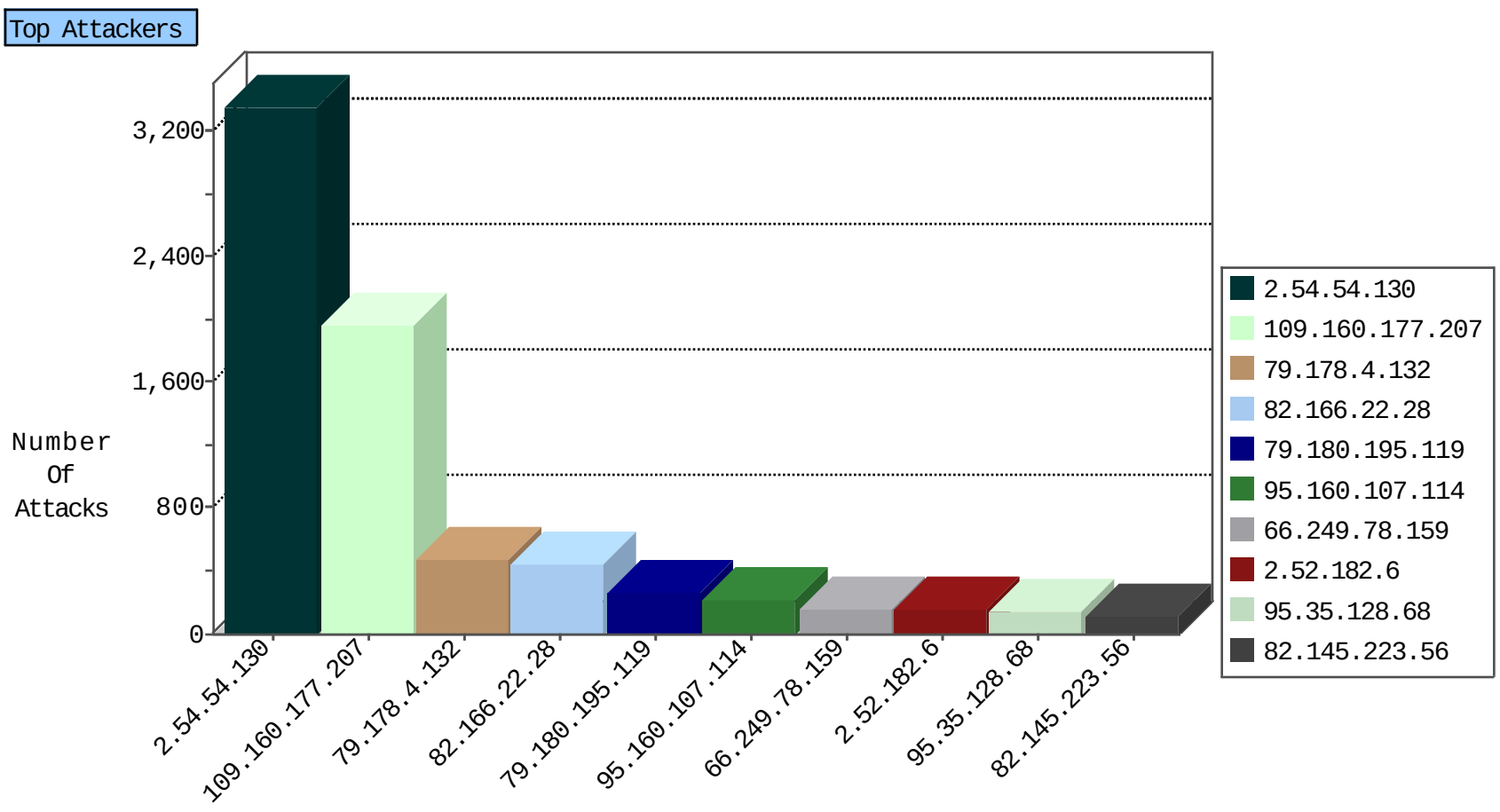
10-21-2015-21:04:04 to 10-21-2015-22:04:04

IDF Under Attack Daily Report





10-21-2015-21:04:04 to 10-21-2015-22:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3074
52.21.115.243	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	113
109.66.30.72	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	19
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	17
46.19.86.238	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	12
95.35.128.68	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
212.150.214.90	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
80.246.136.238	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.59.33.250	Sweden	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
95.35.128.68	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
79.176.24.71	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.70	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
10.0.0.1		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
77.125.98.120	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
93.85.115.69	Belarus	147.237.76.39	mobile.meitav.idf.i	Block_Udp_All_Nets	drop	2
82.221.105.7	Iceland	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
37.46.39.160	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
84.111.38.37	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
38.229.1.13	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
5.43.218.183	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-21-2015-21:04:04 to 10-21-2015-22:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

10-21-2015-21:04:04 to 10-21-2015-22:04:04

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	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
218.108.132.58	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.77.235	Turkey	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
197.164.51.84	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
158.85.158.198	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.67.134	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1

10-21-2015-21:04:04 to 10-21-2015-22:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.54.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3344
109.160.177.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1974
79.178.4.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	479
82.166.22.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	446
79.180.195.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	268
95.160.107.114	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	221
2.52.182.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	159
95.35.128.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	138
82.145.223.56	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	118
141.0.15.120	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	78
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
79.181.120.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	74
82.145.217.208	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	71
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
176.18.8.93	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
5.43.218.183	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
141.0.15.26	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
46.120.14.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
37.46.39.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
23.27.220.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
100.38.183.54	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
176.13.2.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
79.181.9.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
176.205.69.3	United Arab Emirates	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
12.249.99.202	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
176.12.138.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
213.139.52.31	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
92.241.55.190	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
5.22.130.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
168.63.139.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
105.108.53.209	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
2.54.6.23	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
149.88.145.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
109.64.21.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
37.231.135.0	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
46.19.86.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
37.26.146.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
75.39.29.143	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
46.19.86.72	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	84
109.66.108.76	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	70
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
66.249.93.203	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	42
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	42
109.160.168.149	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
46.19.85.127	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
188.143.232.16	Russian Federation	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
46.19.86.17	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.17	Block	28
66.249.93.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	28
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
185.32.179.155	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
79.182.107.81	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	14
171.7.37.75	Thailand	147.237.77.216	dover.idf.il	eMail Hoarding	Block	14
84.228.254.197	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	14
79.178.124.191	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	14
149.88.119.204	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
46.116.201.148	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.116.201.148	Block	14
66.249.93.207	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	14
176.9.58.227	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/shared/usercontrols/headerupper/	Block	14
46.19.85.139	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	14
98.158.127.36	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
79.178.180.7	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	14
207.46.13.119	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
46.116.201.148	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/https:/aka.idf.il/	Block	14
31.210.177.232	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/chinuch/klali/	None	14
79.183.132.196	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/print_text.asp	Block	14
176.13.2.224	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	14
46.19.85.174	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	14
79.181.104.126	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	14
209.181.115.17	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	14
168.63.139.43	United States	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 168.63.139.43	Block	14
46.116.250.69	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	14
38.111.147.84	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
82.221.105.7	Iceland	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	14
180.153.180.121	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/scriptresource.axd%3fd	Block	14
109.66.164.194	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	14
79.182.3.178	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
213.57.225.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	14
171.7.37.75	Thailand	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	14
46.120.130.103	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	14
46.19.85.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
84.108.94.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
78.128.92.193	Bulgaria	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	14
157.55.39.66	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8855-he/navy.aspx	Block	11