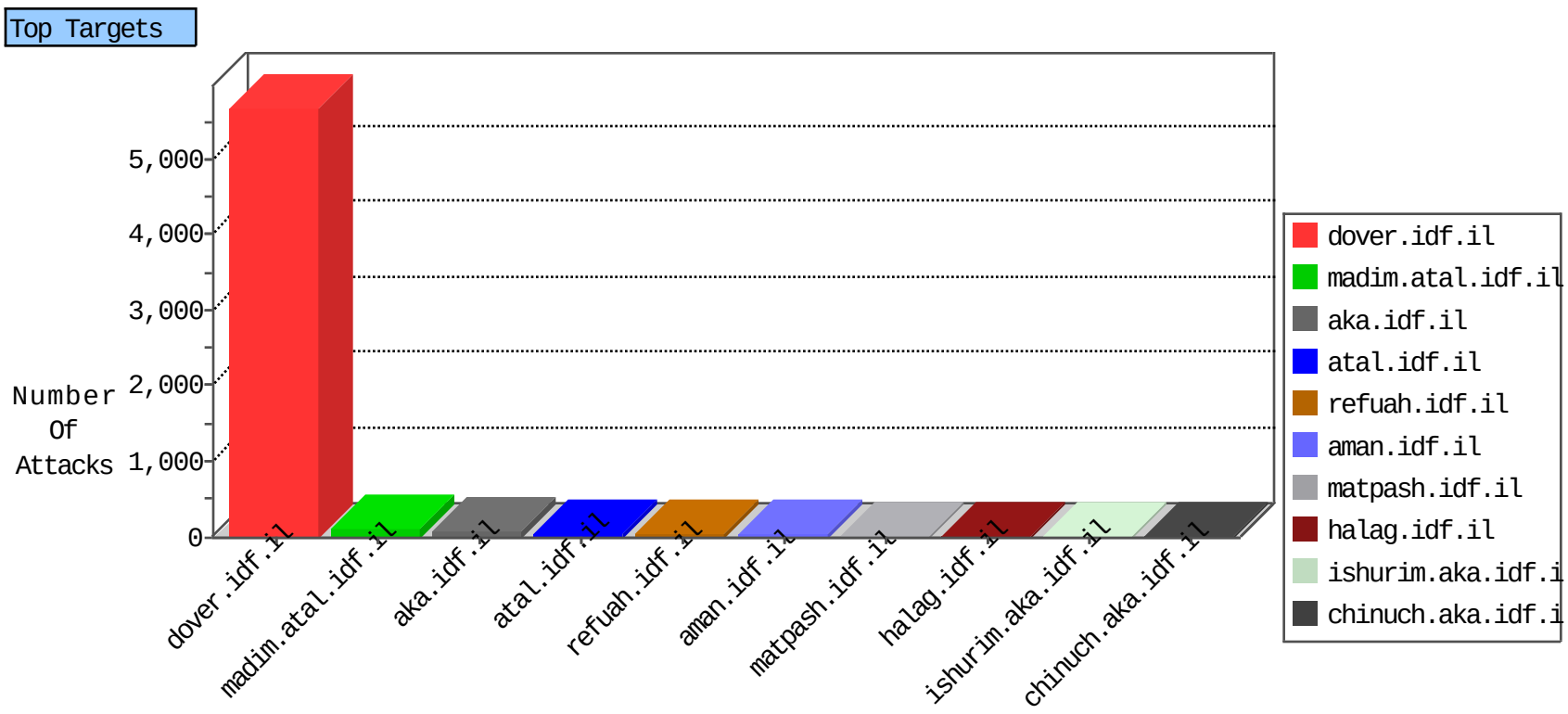
11-06-2015-23:04:00 to 11-07-2015-00:04:00

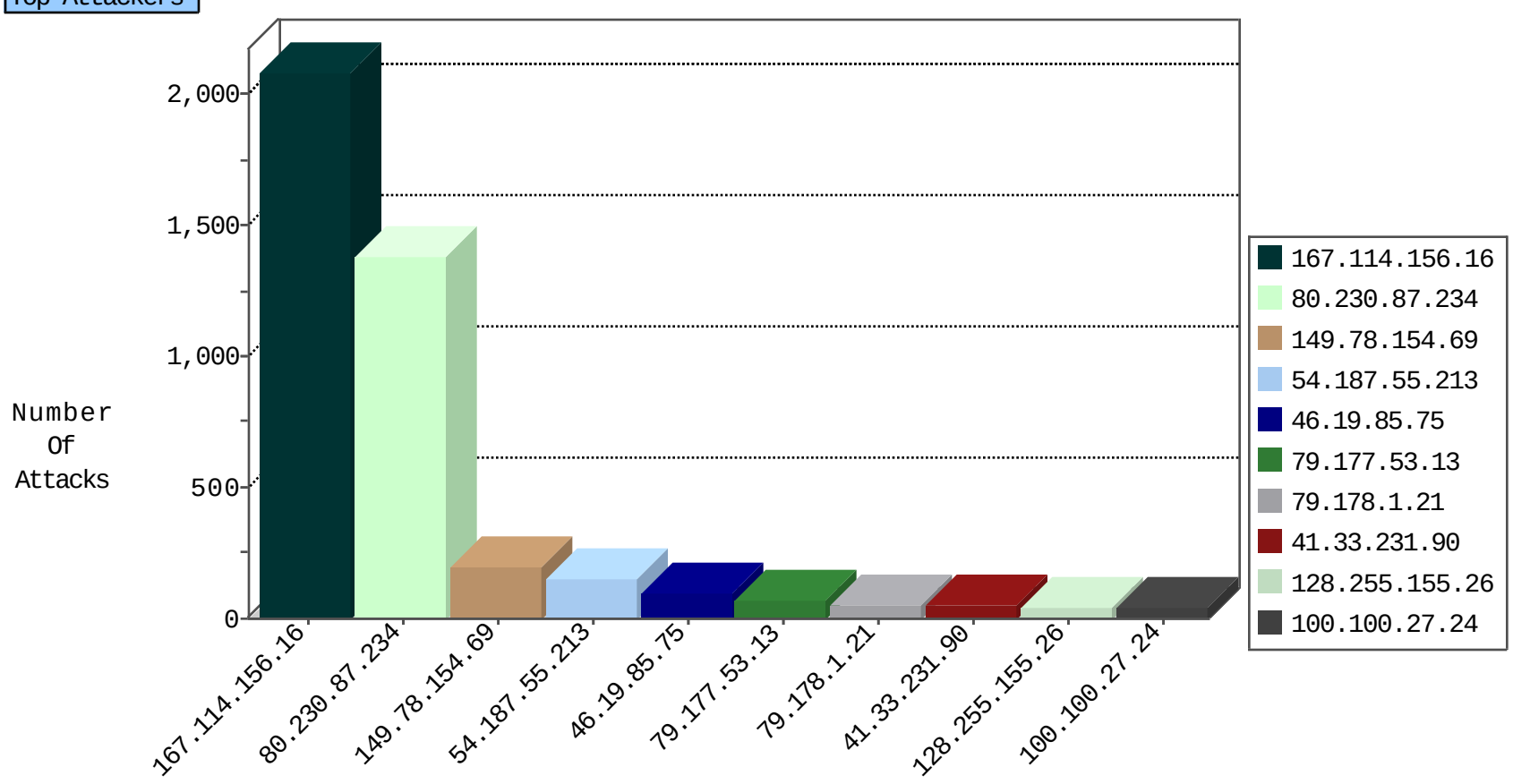
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-06-2015-23:04:00 to 11-07-2015-00:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.208	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	8283
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3303
220.181.108.92	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	209
66.249.67.200	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	193
212.199.95.73	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
108.250.9.127	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
176.12.141.55	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
86.108.81.116	Jordan	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.7.59	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.7.59	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
70.214.6.90	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
66.249.65.198	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
93.168.76.231	Romania	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
71.6.158.166	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
167.114.82.227	Canada	147.237.76.200	eitan.aka.idf.i	Block_Udp_All_Nets	drop	1
5.8.66.69	Russian Federation	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

11-06-2015-23:04:00 to 11-07-2015-00:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-06-2015-23:04:00 to 11-07-2015-00:04:00

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
176.13.0.219	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.67.244	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.191	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.75.214	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
104.128.144.131	147.237.76.200	Canada	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
85.106.4.54	147.237.8.45	Turkey	e.eitan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
222.186.21.25	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.21.25	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
197.157.244.243	147.237.77.178	Somalia	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
5.8.66.110	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN Potential SSH Scan	1
190.88.160.239	147.237.77.176	Netherlands Antilles	matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
188.138.9.51	147.237.72.167	Germany	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
119.73.228.136	147.237.0.19	Singapore	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
89.248.174.106	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.25	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.67.240	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
222.186.21.25	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.179.35.226	147.237.77.216	Australia	dover.idf.il	Xenu Link Sleuth User Agent	1
202.198.75.232	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
14.162.114.40	147.237.0.34	Vietnam	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
188.138.9.51	147.237.77.234	Germany	halag.idf.il	ET SCAN NMAP -sS window 1024	1

11-06-2015-23:04:00 to 11-07-2015-00:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.230.87.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1381
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	192
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	147
46.19.85.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	97
128.255.155.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
71.99.166.122	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
5.15.55.24	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
46.117.97.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
79.178.1.21	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
46.19.85.124	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
212.199.182.150	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	36
37.26.148.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
84.228.111.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
46.19.86.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
46.116.107.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
2.54.7.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
59.183.27.160	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
174.90.223.113	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
100.100.27.24		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
217.132.227.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.19.85.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
77.126.235.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
93.172.139.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
100.100.27.24		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
212.199.95.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
157.55.39.63	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.86.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
67.189.75.139	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
79.178.1.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
85.68.249.130	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
5.102.254.133	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
176.12.141.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
5.102.254.216	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
176.13.0.219	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
52.25.12.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
207.46.13.127	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
207.46.13.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10

11-06-2015-23:04:00 to 11-07-2015-00:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.53.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
185.32.179.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
79.177.53.13	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.177.53.13	Block	24
79.183.215.105	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.183.215.105	Block	4
37.122.154.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.18.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.30.25.92	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to chinuch.aka.idf.il/404.htm	Block	2
40.77.167.63	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.79.31	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	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/4/2904.pdf	Block	1
108.171.211.74	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
64.19.78.242	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
66.249.64.113	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/8/308.pdf	Block	1
109.65.210.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.67.240	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
199.59.148.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/size220x0/5582.jpg	Block	1
64.79.85.205	United States	147.237.77.170	maarachot.idf.il	URL is Above Root Directory maarachot.idf.il/../	Block	1
79.183.215.105	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
66.249.64.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/4/264.pdf	Block	1
5.102.254.133	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
151.80.31.117	Italy	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
79.178.1.21	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
217.69.136.208	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/yassin1.wmv	Block	1
66.6.46.225	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22901-he/dover.aspx#.vj0gus_34lg.tumblr	Block	1
80.246.136.165	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
74.217.148.72	United States	147.237.72.166	aka.idf.il	Abnormally Long Request request version	Block	1
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
79.180.57.139	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.25	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2907.pdf	Block	1
85.250.54.170	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
74.217.148.72	United States	147.237.72.166	aka.idf.il	Illegal HTTP Version browser_broker.exe HTTP/1.1	Block	1
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
79.183.215.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	1

11-06-2015-23:04:00 to 11-07-2015-00:04:00