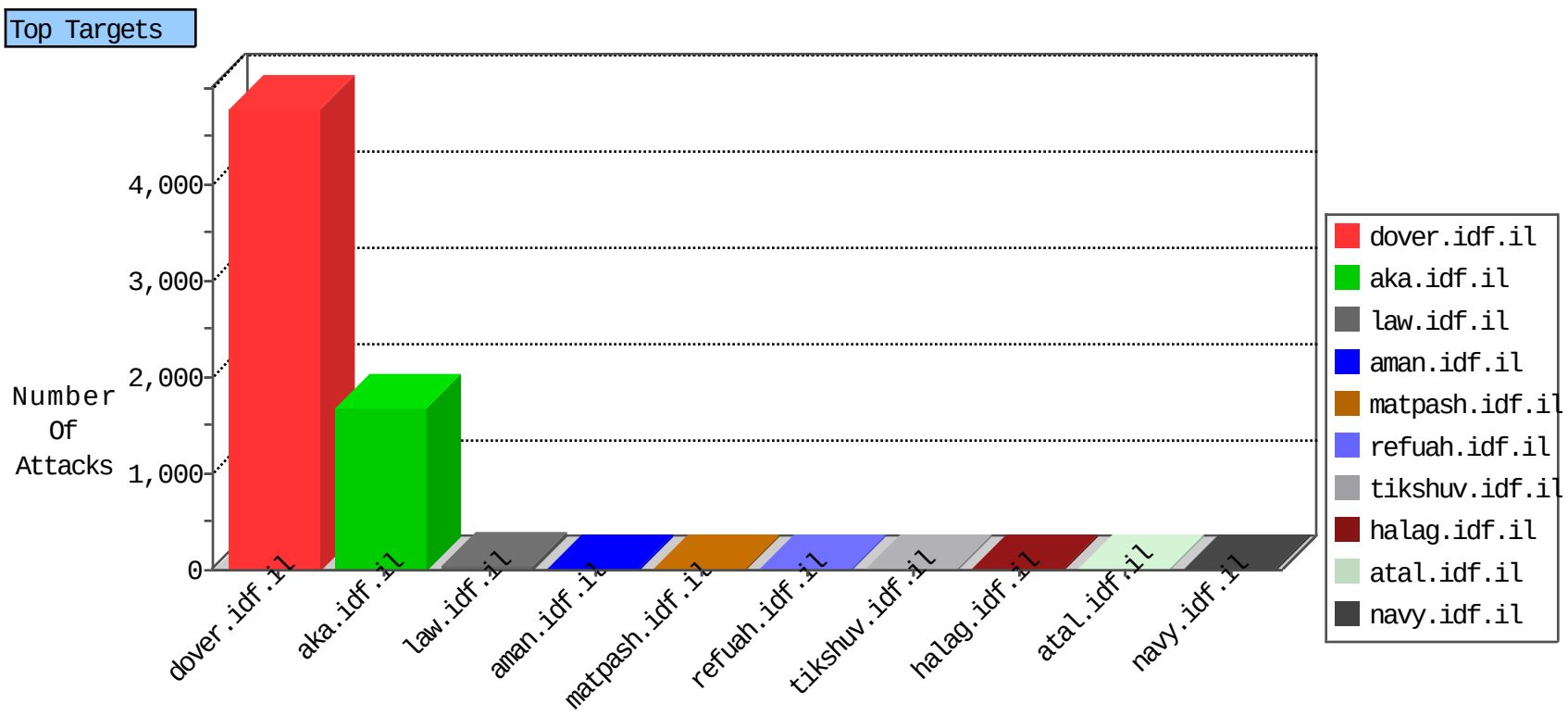
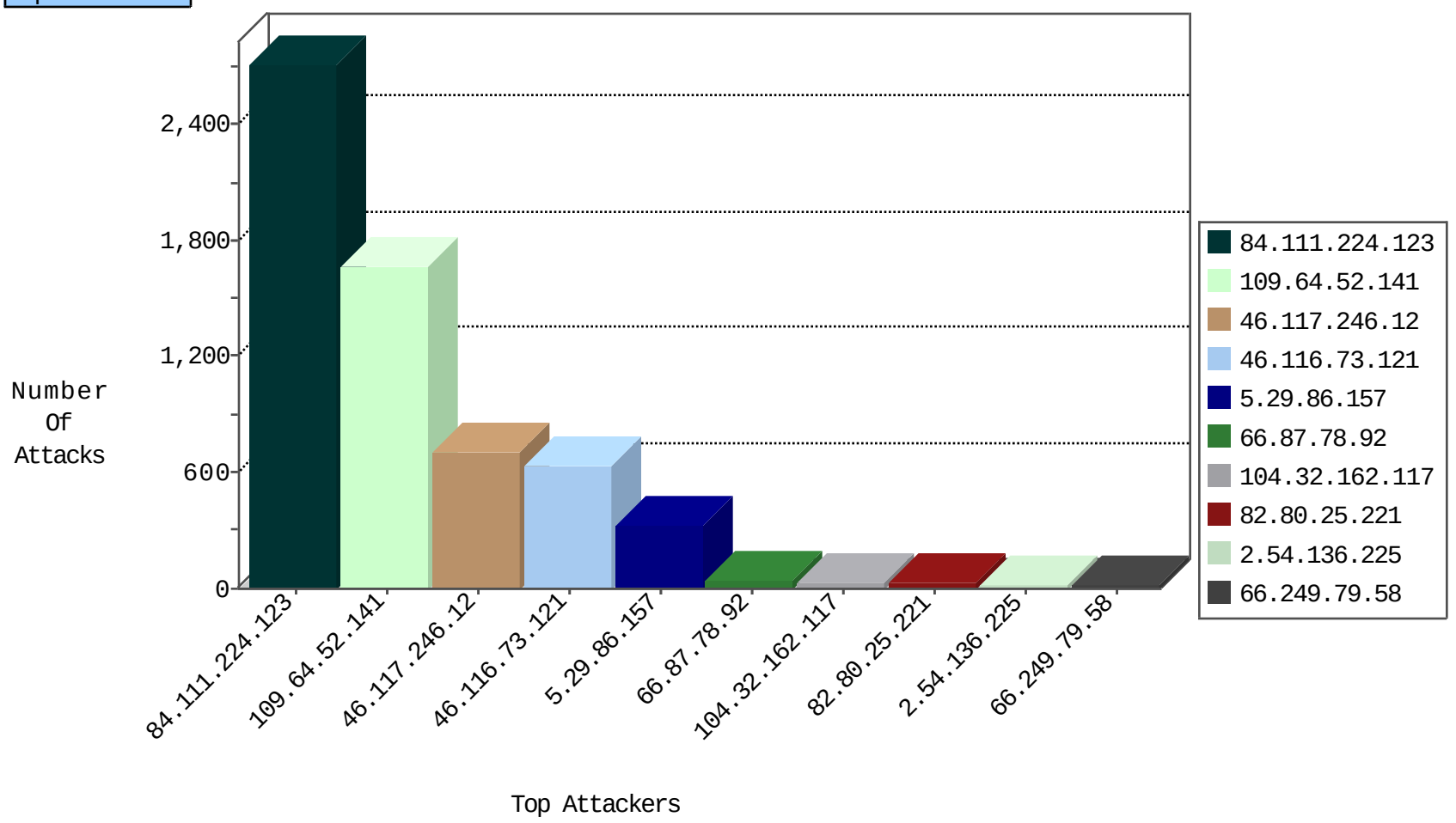
04-24-2015-20:03:02 to 04-24-2015-21:03:02

IDF Under Attack
04-24-2015-20:03:02

Top Targets



Top Attackers



04-24-2015-20:03:02 to 04-24-2015-21:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
207.35.33.164	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9381
100.33.79.215	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7696
109.64.42.16	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5685
82.145.222.142	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5382
207.46.13.52	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2732
109.186.33.116	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2618
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	438
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	370
2.54.136.225	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	124
220.181.108.111	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	64
220.181.108.171	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
200.122.139.69	Costa Rica	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
89.248.171.221	Netherlands	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
113.108.21.16	China	147.237.0.35	akaws.idf.il	L4 Source or Dest Port Zero	drop	1
146.185.239.100	Russian Federation	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
86.186.138.187	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.86.129	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
87.68.70.8	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.199.182.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-24-2015-20:03:02 to 04-24-2015-21:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.64.52.141	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	1675
46.120.128.121	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
198.7.238.40	United States	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
187.174.132.90	Mexico	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
37.142.186.37	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
80.187.108.51	Germany	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.79	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
74.103.245.18	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1

04-24-2015-20:03:02 to 04-24-2015-21:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	28
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
46.116.163.145	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
220.248.17.110	China	147.237.8.14	e.orchot.idf.il	GPL SCAN nmap TCP	2
180.169.108.158	China	147.237.8.14	e.orchot.idf.il	GPL SCAN nmap TCP	2
43.255.191.163	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
114.112.96.133	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.132.118	Russian Federation	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
58.253.96.122	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.163	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
114.112.96.133	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
113.21.226.56	New Zealand	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
89.40.71.178	Romania	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
77.125.132.63	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.183.128.6	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
58.253.96.122	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
218.6.132.45	China	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.163	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1

04-24-2015-20:03:02 to 04-24-2015-21:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
84.111.224.123	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2717
46.117.246.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	712
46.116.73.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	634
5.29.86.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	322
66.87.78.92	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
66.250.99.179	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
198.7.238.40	United States	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	9
85.96.160.254	Turkey	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
176.12.142.247	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
187.174.132.90	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
54.245.64.111	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	7
109.64.173.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
5.11.46.149	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.67.104	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
85.72.40.4	Greece	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
79.182.53.153	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.79.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.86.225	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
69.116.53.67	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
79.175.206.128	Poland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
79.176.227.46	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
109.253.128.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
79.182.29.110	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
85.65.143.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.43.125.12	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
37.26.147.193	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.43.125.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.79.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
12.199.98.27	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
84.229.131.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
79.177.103.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.64.209.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.142.135.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.250.94.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.229.175.96	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
149.78.43.220	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.86.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.181.31.91	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.253.130.78	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.65.198.132	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.177.179.40	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

04-24-2015-20:03:02 to 04-24-2015-21:03:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
104.32.162.117		147.237.77.74	law.idf.il	PHP Attempt	Block	15
104.32.162.117		147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 104.32.162.117	Block	14
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	9
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	4
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	3
80.246.133.160	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
157.55.39.8	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
17.228.4.80	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.228.4.80	Block	2
93.172.169.104	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
67.186.32.148	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	2
157.55.39.5	United States	147.237.72.166	aka.idf.il	Unknown Parameter pageNum in www.aka.idf.il/patzar/klali/default.asp	None	1
2.54.50.253	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/894-he/refuah.aspx	Block	1
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
38.111.147.84	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
66.249.65.157	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1238-he/atal.aspx	Block	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/november/23z.stm	Block	1
84.109.152.29	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/eitan/listpage/default.asp	None	1
46.117.194.149	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/giyus	Block	1
157.55.39.205	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1392-he/refuah.aspx	Block	1
77.127.170.100	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.178	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on 147.237.77.74//	Block	1
157.55.39.13	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1638-he/refuah.aspx	Block	1
17.228.4.80	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
85.65.48.250	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.120.128.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
157.55.39.244	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
104.32.162.117		147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/321-en/text/javascript	Block	1
79.177.141.247	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
66.249.73.158	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/m/	Block	1
157.55.39.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/personalentrance.asp	Block	1
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.81.230	Israel	147.237.77.176	matpash.idf.il	URL is Above Root Directory www.cogat.idf.il/../favicon.ico	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	1
188.165.15.13	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.13	Block	1
109.64.221.61	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
80.230.70.86	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.173	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8688-he/refuah.aspx	Block	1
37.142.213.97	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
94.153.10.19	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/+	Block	1
66.249.65.153	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1240-he/atal.aspx	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/site- ØªØ§Ø±ÙŠØ® Ø§Ù„ Ø¯ØªÙˆÙ„ 2-12-2004	Block	1

04-24-2015-20:03:02 to 04-24-2015-21:03:02