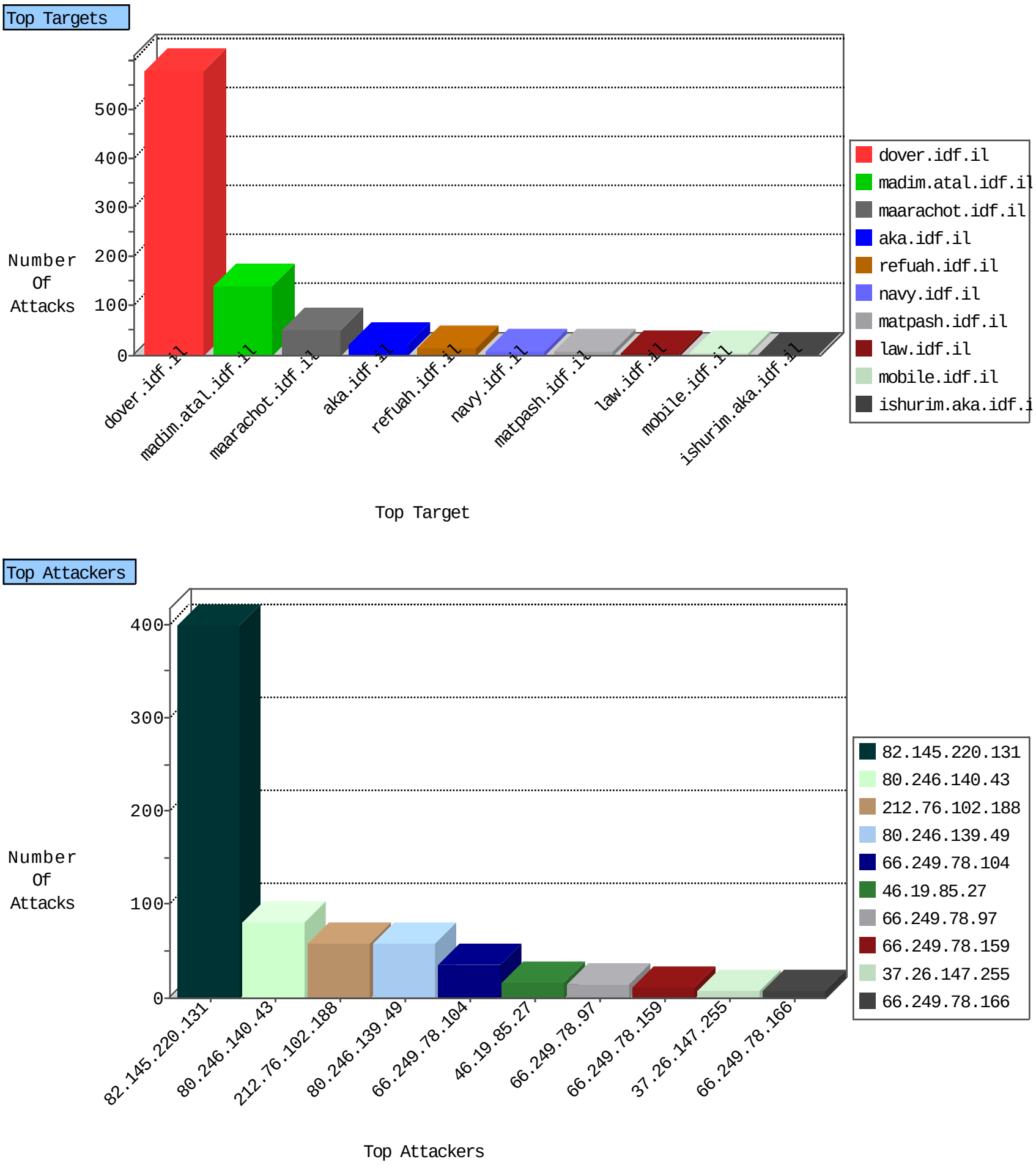
04-26-2015-00:03:02 to 04-26-2015-01:03:02

IDF Under Attack
04-26-2015-00:03:02



04-26-2015-00:03:02 to 04-26-2015-01:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2571
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	865
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	808
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	298
220.181.108.84	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	29
109.67.198.216	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	17
66.249.78.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
66.249.78.111	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1

04-26-2015-00:03:02 to 04-26-2015-01:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
107.170.68.76	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
109.66.146.133	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
198.20.69.98	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1

04-26-2015-00:03:02 to 04-26-2015-01:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	34
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
176.43.145.15	Turkey	147.237.77.216	dover.idf.il	INDICATOR-OBFUSCATION script tag in POST parameters - likely cross-site scripting	2
66.249.78.159	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.59	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
218.3.243.223	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.3.243.223	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
2.83.238.191	Portugal	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
208.184.217.221	United States	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 3072	1
2.83.238.191	Portugal	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
81.200.91.2	Russian Federation	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
218.3.243.223	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
2.83.238.191	Portugal	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
212.199.182.150	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
2.83.238.191	Portugal	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
176.12.138.78	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
81.200.91.2	Russian Federation	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 4096	1

04-26-2015-00:03:02 to 04-26-2015-01:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.145.220.131	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	400
212.76.102.188	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
37.26.147.255	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
86.42.55.244	Ireland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.85.27	Israel	147.237.76.42	refuah.idf.i	Invalid ACK number	Bad TCP sequence	alert	6
46.19.85.27	Israel	147.237.76.42	refuah.idf.i	Invalid ACK number	Bad TCP sequence	monitor	6
176.12.150.51	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
94.230.86.230	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
79.180.168.16	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
2.54.17.17	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
176.12.145.85	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
77.127.232.70	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.27	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
207.46.13.95	United States	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
84.111.25.175	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.27	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
98.228.54.35	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
80.246.133.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.110.57.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
77.127.232.206	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
141.212.121.194	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
68.198.141.50	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.85.84	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
220.181.108.167	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
109.64.42.16	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.220.158.116	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
176.12.150.51	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
87.68.214.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
77.125.95.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.86.228	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
24.2.247.164	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
109.66.60.228	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
87.160.199.128	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
50.78.45.121	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
24.2.247.164	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
128.232.110.28	United Kingdom	147.237.76.196	e.sviva.idf.	Geo-location inbound enforcement	Geo-location enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
80.246.140.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	82
80.246.139.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	58
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	4
84.111.155.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
2.54.160.18	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.160.18	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
80.246.137.96	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
2.54.160.18	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
94.153.66.163	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	2
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//newsite/hebrew/main.stm	Block	1
46.19.86.74	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
176.12.150.219	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
85.131.77.116	Finland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/march/31.stm	Block	1
71.165.11.130	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.stm	Block	1
200.29.126.154	Colombia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/simbolos judios	Block	1
66.249.64.61	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/smalim/showbig.aspx	Block	1
104.32.162.117		147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il./	Block	1
46.116.2.222	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
180.76.4.60	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
89.138.226.221	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ie-contacts.stm	Block	1
66.249.67.58	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/armored7.stm	Block	1
109.65.188.75	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/navmenu/undefined	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
46.119.113.155	Ukraine	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//	Block	1
80.246.130.169	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.66	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/shvuim.stm	Block	1
37.8.27.230	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1206-en/cogat.aspxcoordination	Block	1
188.165.15.94	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/giyus.asp	Block	1
46.121.247.55	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
94.159.130.143	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.133.176	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/ordnance/ordnance.stm	Block	1
46.19.85.176	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
85.64.189.76	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0403-3.stm	Block	1
192.171.235.80	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/entebbe2.stm	Block	1
54.161.135.168	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/021022-2.stm	Block	1
95.86.73.123	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1

04-26-2015-00:03:02 to 04-26-2015-01:03:02