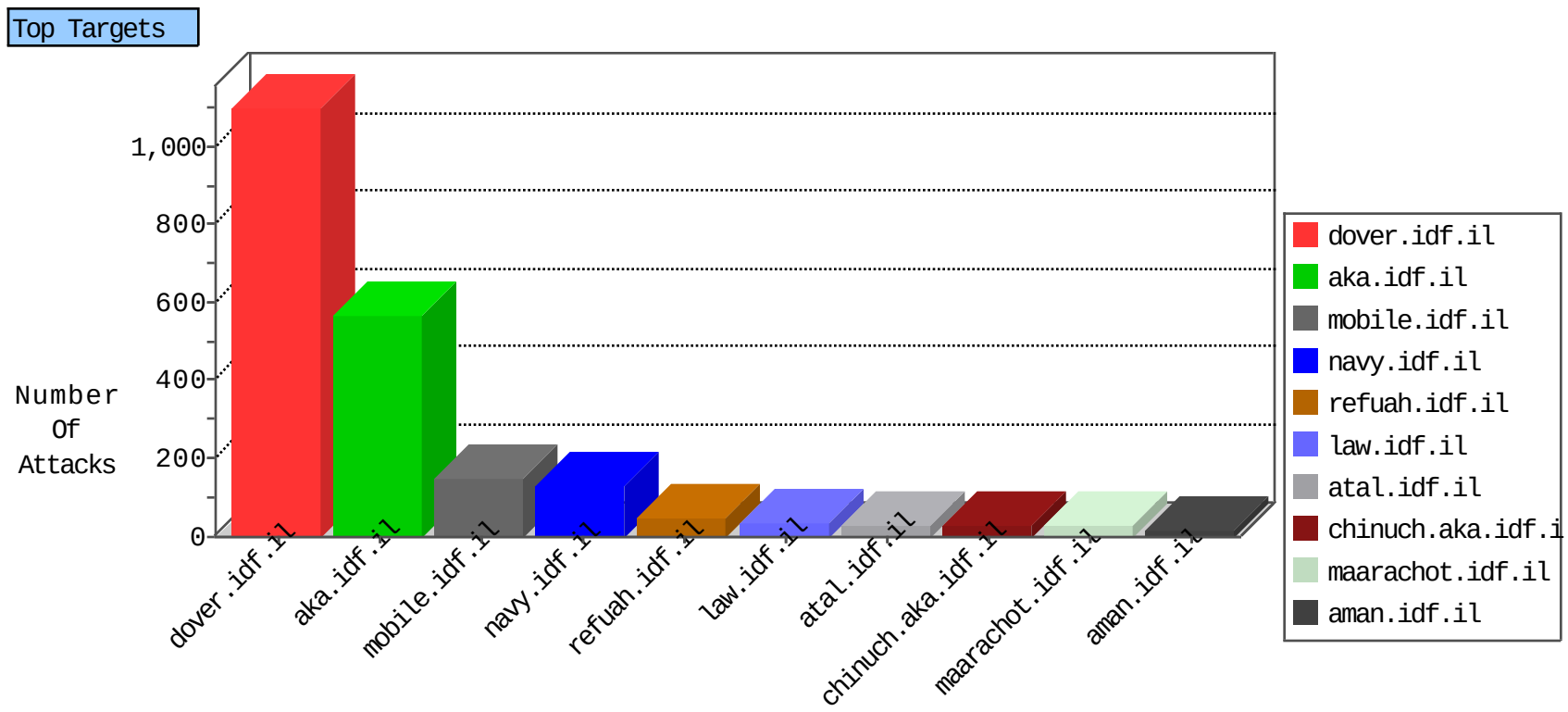
10-31-2015-00:04:00 to 10-31-2015-01:04:00

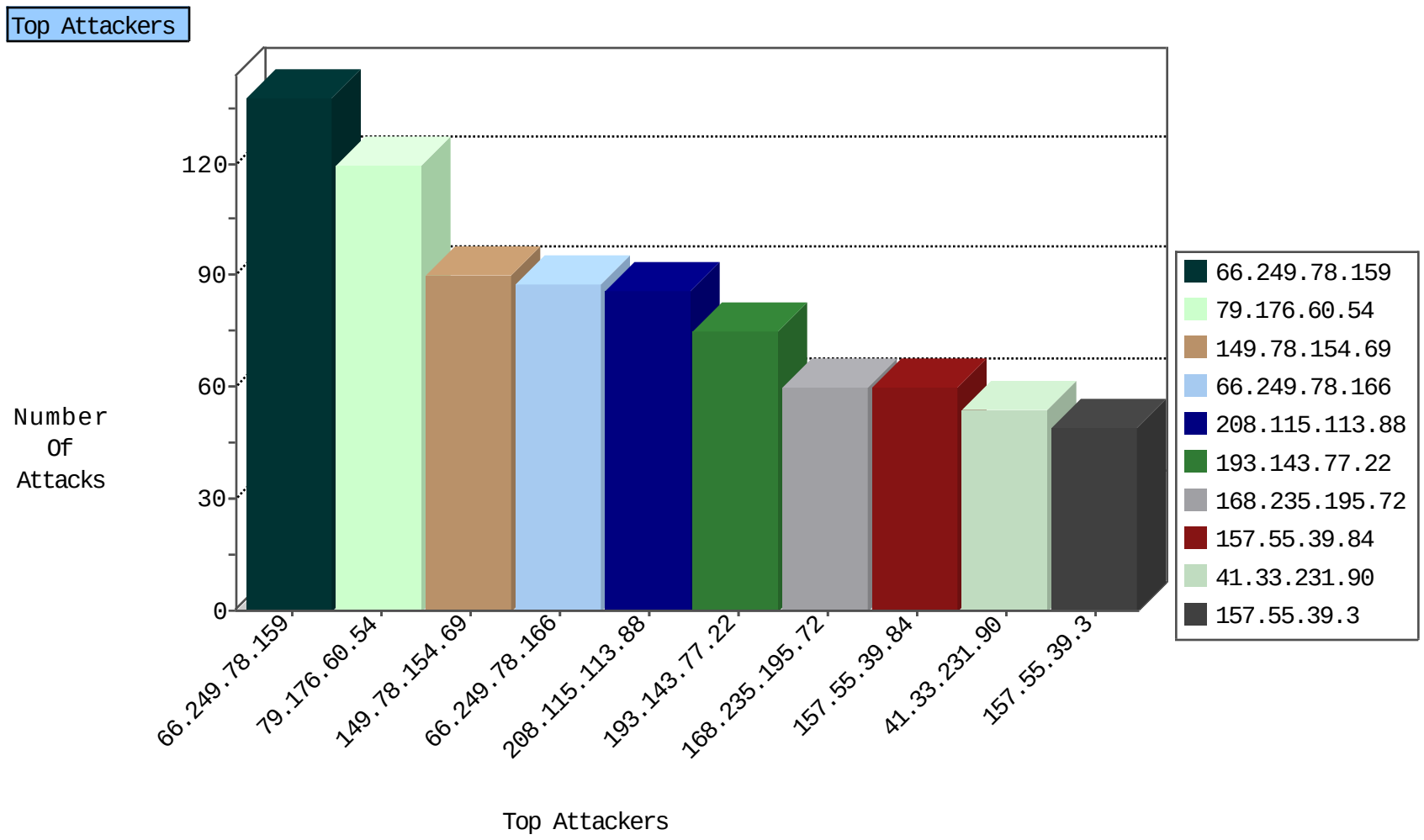
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-31-2015-00:04:00 to 10-31-2015-01:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.75.68	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4180
66.249.69.76	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3132
173.84.92.52	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	955
66.249.67.20	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	358
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	217
149.78.154.69	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	180
154.72.174.197	Cameroon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	89
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	65
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	54
145.53.254.110	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	20
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
66.249.84.187	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6
66.249.84.188	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
212.179.227.147	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
170.149.100.10	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
134.147.203.115	Germany	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	4
37.26.148.136	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
80.246.136.194	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
37.8.46.154	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
134.147.203.115	Germany	147.237.76.38	e.e.meitav.idf.i	Block_Ntp_All_Net	drop	2
86.128.79.238	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
154.72.174.197	Cameroon	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
188.138.9.50	Germany	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

10-31-2015-00:04:00 to 10-31-2015-01:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
78.25.120.42	Russian Federation	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1

10-31-2015-00:04:00 to 10-31-2015-01:04:00

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	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.75.2	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
59.45.79.117	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
199.101.186.159	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
197.225.31.39	147.237.76.38	Mauritius	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
169.57.5.20	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
169.57.5.20	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
61.7.181.51	147.237.77.179	Thailand	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
61.7.181.51	147.237.77.179	Thailand	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
200.195.135.82	147.237.76.44	Brazil	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.76.30	United States	himush.idf.il	ET DROP Dshield Block Listed Source	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
169.57.5.20	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
61.7.181.51	147.237.77.179	Thailand	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1

10-31-2015-00:04:00 to 10-31-2015-01:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
31.173.80.21	Romania	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
173.84.92.52	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	21
166.170.0.126	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
108.61.122.218	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
66.249.84.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
100.100.73.230		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
84.228.242.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.73.230		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.106.227.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.164.132.119	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
86.128.79.238	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
31.186.228.32	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.36	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
31.186.228.93	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.231	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.180.9.72	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.78.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
31.186.228.96	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.166.22.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.186.228.60	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.186.228.57	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.4.10.6	Germany	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	6
31.186.228.95	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
82.17.243.170	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.108.14.143	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
31.210.186.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.60.54	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	120
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	75
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	75
193.143.77.22	Poland	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 193.143.77.22	Block	60
79.170.40.38	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.170.40.38	Block	45
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	45
168.235.195.72	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 168.235.195.72	Block	45
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	30
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	30
2.54.167.247	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.69.84	Israel	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	15
157.55.39.84	United States	147.237.72.166	aka.idf.il	Unknown Parameter newsitem in aka.idf.il/chinuch/news/default.asp	None	15
145.255.140.215	Russian Federation	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1283-19111-en/dover.aspx	Block	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/smalim/showbig.aspx	Block	15
66.249.79.228	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.79.228	Block	15
176.106.227.36	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17890-he/dover.aspx	Block	15
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in aka.idf.il/iturim/asp/wars.asp	None	15
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
46.19.85.158	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	15
66.249.73.194	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/eitan/listpage/	Block	15
157.55.39.106	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	15
151.25.230.40	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https:/twitter.com/	Block	15
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/see	Block	15
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.79.235	Block	15
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17032-he/dover.aspx	Block	15
66.249.67.243	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/default.asp	Block	15
157.55.39.84	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/sites/miktzoa/default.asp	None	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.67.6	Block	15
84.111.104.217	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 84.111.104.217 (Open Mode)	None	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-18362	Block	15
66.249.75.54	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	15
157.55.39.214	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/june10a.stm)	Block	15
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	15
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8911-he/refuah.aspx	Block	15
193.143.77.22	Poland	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	15
66.249.67.247	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71733-he/maarachot.aspx	Block	15
157.55.39.84	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/tizmoret/klali/default.asp	None	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1152-he/chinuch.aspx	Block	15
84.111.104.217	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	15
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	15
66.249.78.52	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	15
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chamatz/klali/default.asp	None	15
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	15
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
157.55.39.84	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/edim/fund/funddesc.asp	None	15
84.111.233.28	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	15
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1148-he/chinuch.aspx	Block	15