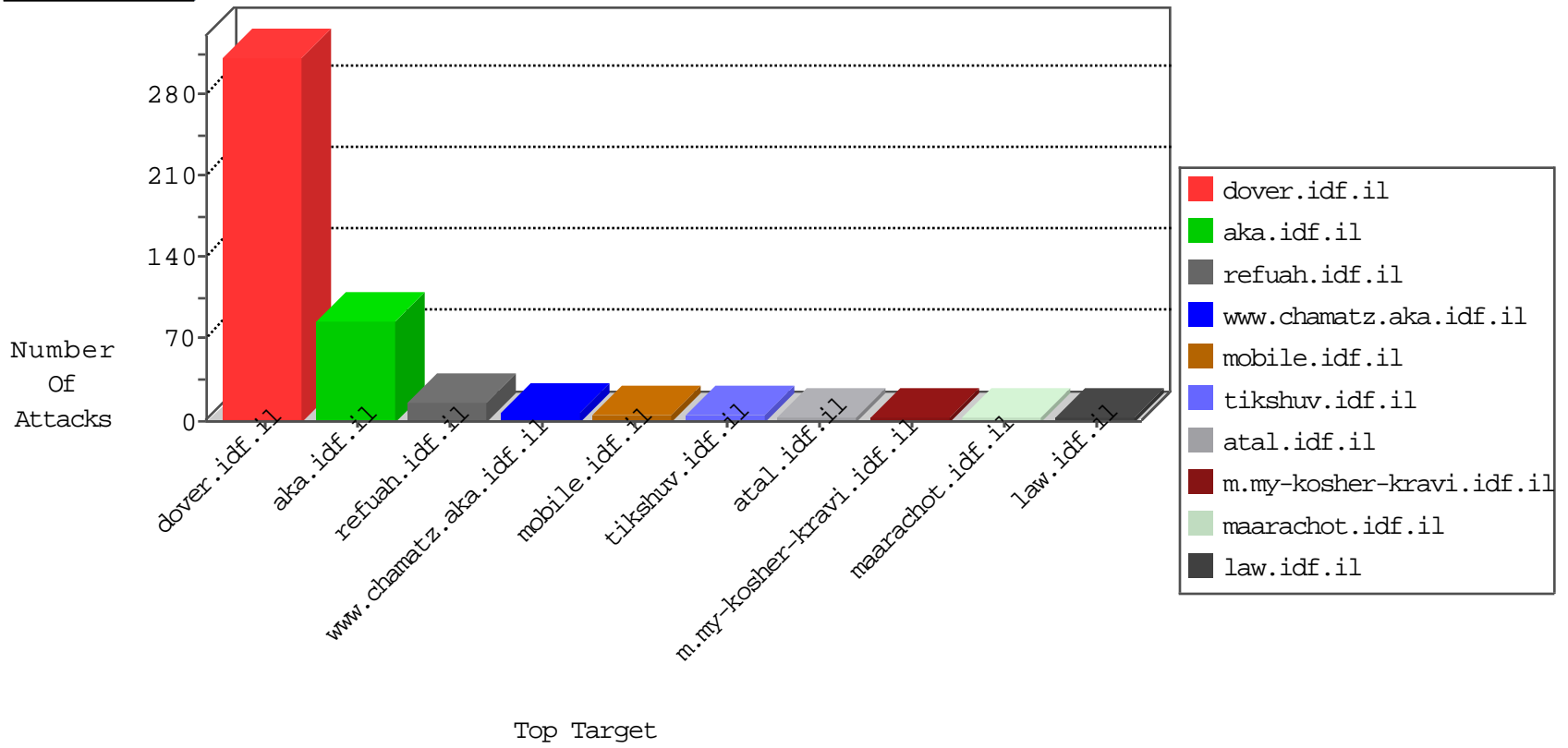


# IDF Under Attack

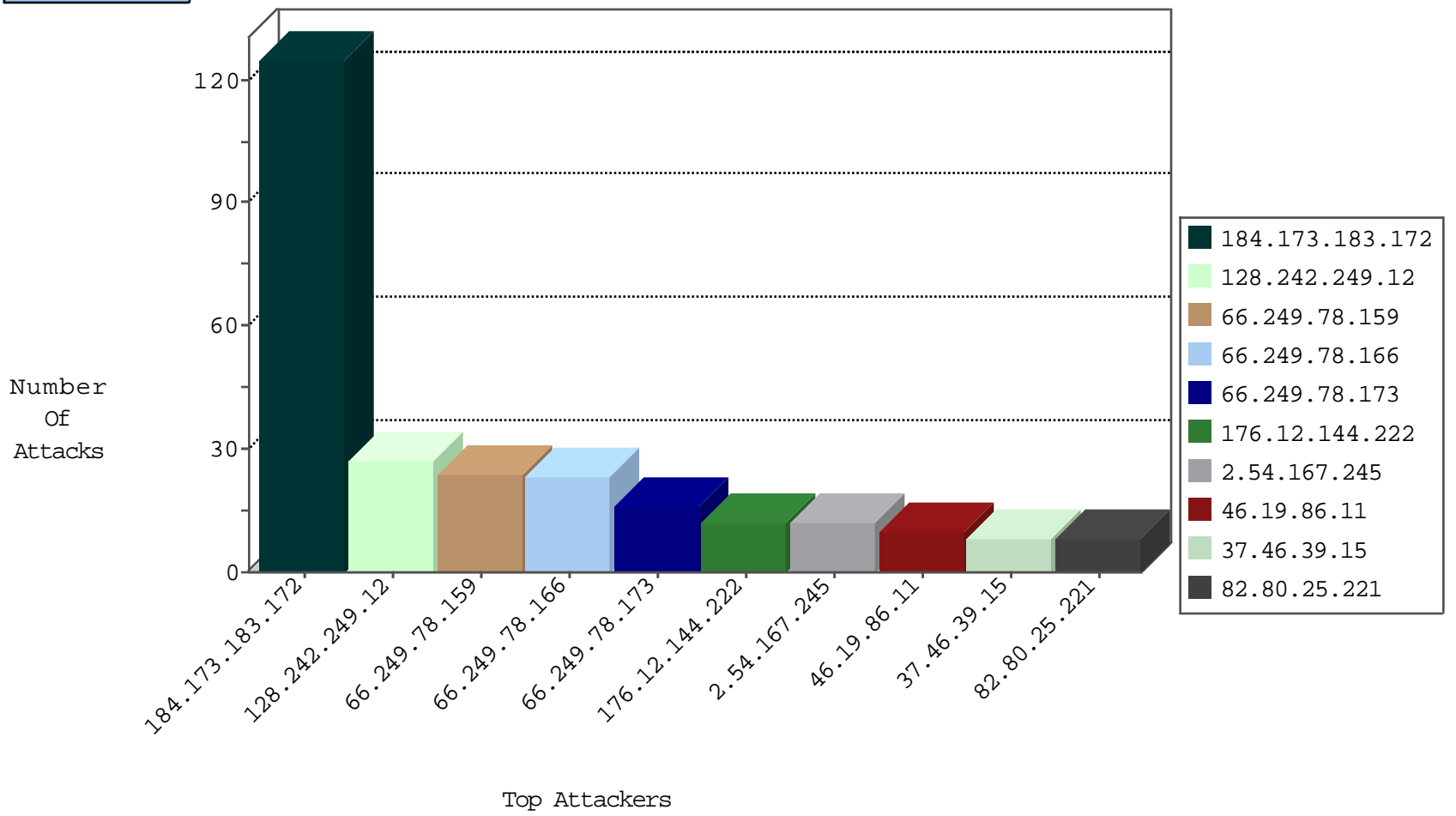
03-29-2015-00:03:03



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
------------------	------------------	----------------	----------	-----------	---------------	-------

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	125
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	27
93.173.242.210	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.25.43.94	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
109.253.144.149	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
85.64.203.171	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
109.253.145.62	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
31.210.178.140	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
109.253.135.136	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
85.25.43.94	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
109.253.136.249	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

## 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	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
5.29.130.33	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.12.137.30	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
218.240.7.91	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.65	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
184.63.28.227	United States	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	1
115.231.218.147	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
85.114.141.217	Germany	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.235	sviva.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.65	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
218.240.7.91	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
211.138.34.58	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
193.107.17.72	Russian Federation	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
89.138.252.139	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
85.114.141.217	Germany	147.237.0.17	m.ny-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
176.12.144.222	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
46.19.86.11	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	10
109.253.146.67	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
37.46.39.15	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
66.249.75.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.137.232	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
2.54.167.245	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
2.54.167.245	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
76.109.47.51	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
2.54.167.245	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	4
94.230.86.128	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
37.46.39.244	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
46.19.85.130	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.178	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.240	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
188.120.148.130	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
37.46.39.15	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
188.120.148.172	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.118	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
77.120.137.10	Ukraine	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
5.102.254.3	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
84.228.215.117	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
188.120.148.245	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
37.142.73.85	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
77.125.140.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.34.162.130	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
84.228.215.117	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
188.165.15.148	France	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
46.19.85.58	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.205	United States	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
77.127.169.77	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
46.116.131.30	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
87.69.100.68	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.64	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.92	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
146.185.239.104	Russian Federation	147.237.8.27	e.madim.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
77.127.169.77	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.117.88.180	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.249	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
37.46.39.63	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.200	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
173.208.203.138	United States	147.237.77.74	law.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
77.237.146.28	Czech Republic	147.237.77.226	www.chamatz.aka.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
46.19.86.5	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
188.120.148.178	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
108.61.122.72	United States	147.237.76.198	e.yohalan.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
95.86.75.3	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	6
31.44.138.118	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	5
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	4
109.253.134.210	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
207.46.13.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.112	Block	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
37.142.104.213	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
5.29.39.144	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	2
80.246.133.12	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
164.138.115.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	2
184.63.28.227	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 184.63.28.227	Block	2
122.59.80.251	New Zealand	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	2
94.159.231.247	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refuah.atal.idf.il/sip_storage/files/0/2950.pdf&ved=0cb0qfjab&usq=afqjcnfrhcnhkt5t7bz2eyz4fvzwd_xs&sig2=5gdk3u4shkicf3tq-7mj1q	Block	2
46.117.82.126	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/home.aspx	None	1
213.57.210.198	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/gyus/authenticationservice.aspx/getuserdetails	Block	1
84.109.2.180	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
188.165.15.148	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.137.232	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.237.207.196	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
109.253.142.60	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/december/25.stm	Block	1
89.138.219.188	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/viewpniot.aspx	None	1
79.182.195.28	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/default.aspx	None	1
184.63.28.227	United States	147.237.77.216	dover.idf.il	XSS - Basic 3	Block	1
66.249.78.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/english/organization/homefront/homefront1.stm	Block	1
157.55.39.6	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0108-3.stm	Block	1
109.64.126.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.117.156.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/drushimw/	Block	1
2.54.17.148	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
84.110.111.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
176.12.149.229	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.120.137.10	Ukraine	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
54.172.196.207	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
109.253.158.204	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.114	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
93.84.1.149	Belarus	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
79.182.195.28	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/payslips.aspx	None	1
188.138.1.218	Germany	147.237.76.39	mobile.meitav.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
157.55.39.41	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/may/16.stm	Block	1
66.249.78.173	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/search.asp	Block	1
109.65.27.161	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
46.120.219.209	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyus/authenticationservice.aspx/getuserdetails	Block	1
201.243.190.160	Venezuela	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
84.111.155.191	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/statistics/gens.stm	Block	1
176.12.150.177	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.237.146.28	Czech Republic	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
113.163.155.149	Vietnam	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
93.171.243.83	Ukraine	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1283-18521-en/dover.aspx	Block	1
46.19.85.37	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/mailbox.aspx	None	1