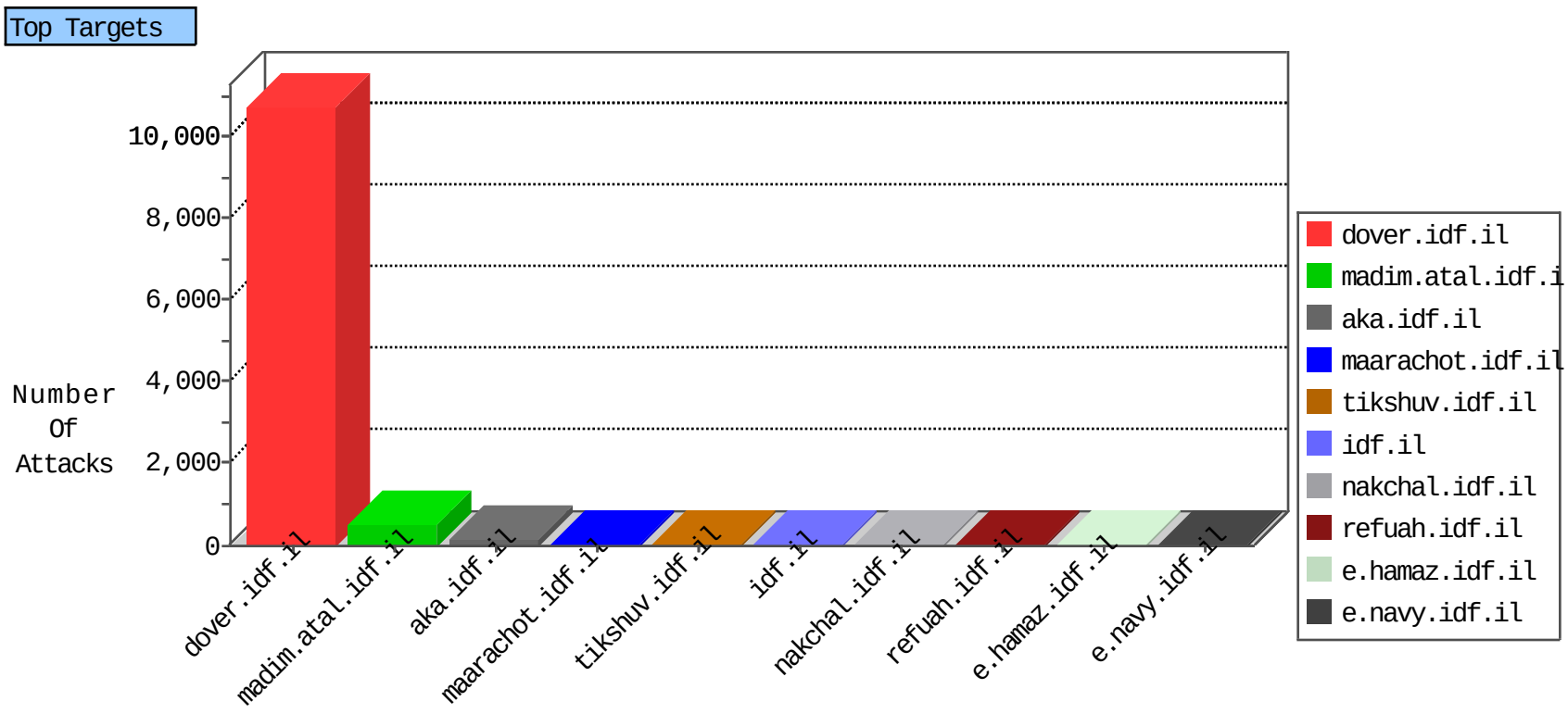
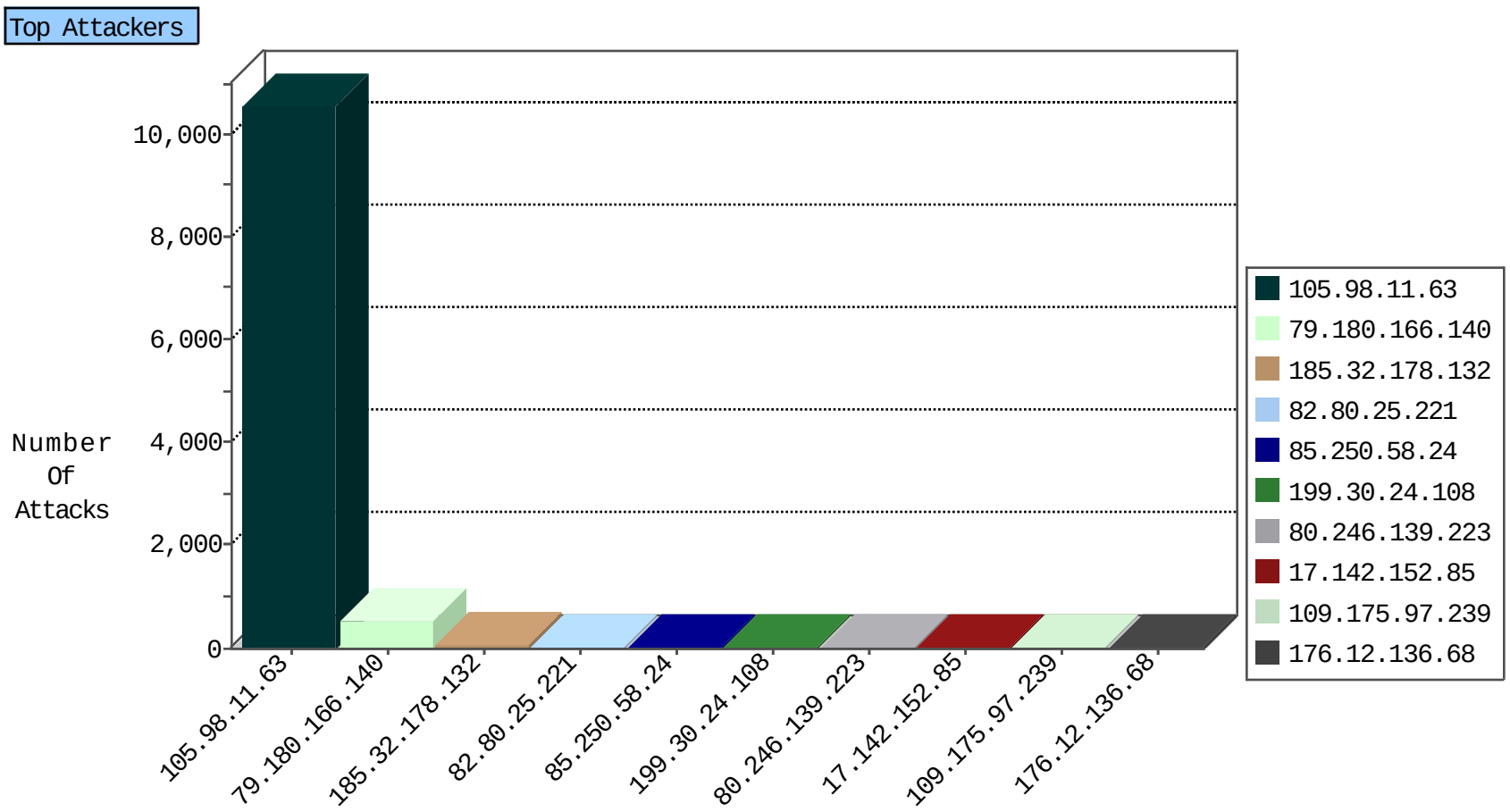
04-01-2015-00:03:07 to 04-01-2015-01:03:07

IDF Under Attack
04-01-2015-00:03:07

Top Targets



Top Attackers



04-01-2015-00:03:07 to 04-01-2015-01:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
37.19.120.119	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
107.154.64.10	United States	147.237.76.196	e.sviva.idf.il	L4 Source or Dest Port Zero	drop	1
89.248.172.57	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.57	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.57	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1

04-01-2015-00:03:07 to 04-01-2015-01:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
105.98.11.63	Algeria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.250.146.221	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
89.110.146.205	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
5.102.254.101	Israel	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	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
109.160.142.144	Israel	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	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1

04-01-2015-00:03:07 to 04-01-2015-01:03:07

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	30
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
222.186.21.201	China	147.237.0.35	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
115.231.218.147	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
115.231.218.147	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
111.203.22.57	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
221.235.188.213	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
128.61.240.66	United States	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
121.42.40.208	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.201	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
121.42.40.208	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.201	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
121.42.40.208	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
115.231.218.147	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.213	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.213	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
111.203.22.57	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.213	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
121.42.40.208	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
121.42.40.208	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
222.186.21.201	China	147.237.76.177	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
121.42.40.208	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

04-01-2015-00:03:07 to 04-01-2015-01:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
105.98.11.63	Algeria	147.237.77.216	dover.idf.il	SAM rule	drop	drop	5576
105.98.11.63	Algeria	147.237.77.216	dover.idf.il		drop	drop	4376
105.98.11.63	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	472
85.250.58.24	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	22
185.32.178.132	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	21
185.32.178.132	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	21
185.32.178.132	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	21
199.30.24.108	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
17.142.152.85	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
109.175.97.239	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	13
65.55.210.71	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.136.68	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
17.142.152.68	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
80.246.139.223	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
80.246.139.223	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
66.249.64.146	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.142.155	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
80.246.139.223	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	6
105.98.11.63	Algeria	147.237.77.216	dover.idf.il	Anonymous DoSer Denial of Service Tool	Web Server Enforcement Violation	reject	6
77.127.119.16	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
46.19.85.186	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
157.55.39.6	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
80.246.137.4	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	3
31.210.186.182	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
94.230.86.252	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
80.246.137.4	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
80.246.137.4	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
85.130.243.118	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2
17.142.152.111	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
2.54.47.172	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
157.55.39.42	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.47.172	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
79.180.166.140	Israel	147.237.0.19	madim.atal.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
37.24.149.199	Germany	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
2.54.47.172	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
17.142.152.86	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.86.240	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
37.24.149.199	Germany	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
17.142.152.94	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
217.132.105.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
141.212.122.31	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
114.112.90.54	China	147.237.0.33	idf.il		drop	drop	1
79.178.132.178	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.31	United States	147.237.76.202	e.halag.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.85.251	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.16	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.180.166.140	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.180.166.140	Block	513
105.98.11.63	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 105.98.11.63	Block	58
105.98.11.63	Algeria	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	57
5.29.31.197	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
105.98.11.63	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type	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
109.186.38.154	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.137.4	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.127.119.16	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl01 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
176.12.144.60	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13437-he/dov	Block	1
5.28.153.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
203.133.169.208	Korea, Republic of	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
79.180.166.140	Israel	147.237.0.19	madim.atal.idf.i	Too Many 404: Response Code per Session	Block	1
66.249.64.150	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.150	Block	1
173.252.79.114	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/sip_storage/files/8	Block	1
109.253.145.237	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.64.125.33	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
176.12.148.154	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.176.125.178	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.112	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.112	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/saudi_arabia/site/english/main_index.stm	Block	1
176.12.136.92	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.159.239	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.58.24	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
185.32.176.150	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
79.177.50.46	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.153	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/main.stm	Block	1
37.142.156.183	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/forgotpassword.aspx	None	1
79.180.166.140	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/mobile/shared/ajax/updatemakatqauntity.aspx	Block	1
176.12.139.49	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.78.103.151	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.138.213.255	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl21 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
185.32.179.54	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.178.120.90	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
159.224.160.225	Ukraine	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112305.pdf++++++++++++++++++++++++++++++++result:+×¡×›×˜×¨×š×ž×œ+×‘×ž×›Ã¼×¨×?Ã¿+×¡×¢ ×?×?×˜×§×š×?,+×?×•+×″×ž×š×?×§×?×?×ž	Block	1
46.120.73.200	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/terms.aspx	None	1
109.65.141.217	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.181.195.118	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
77.127.119.16	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
176.12.141.2	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.17	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/scriptresource.axd	Block	1
2.54.169.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
95.86.69.101	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
203.133.169.208	Korea, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 203.133.169.208	Block	1
79.178.174.136	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.64.142	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.142	Block	1
173.252.79.112	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/sip_storage/files	Block	1