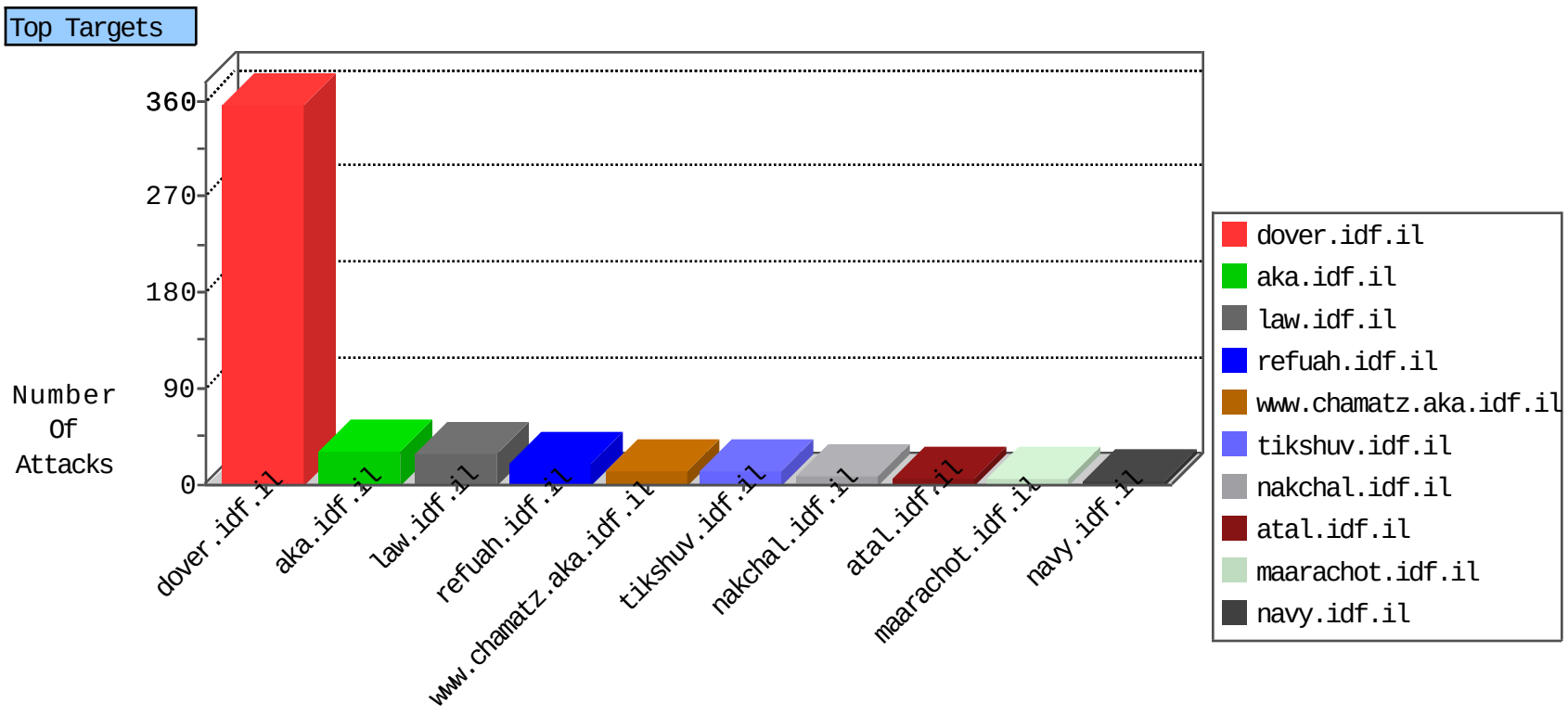
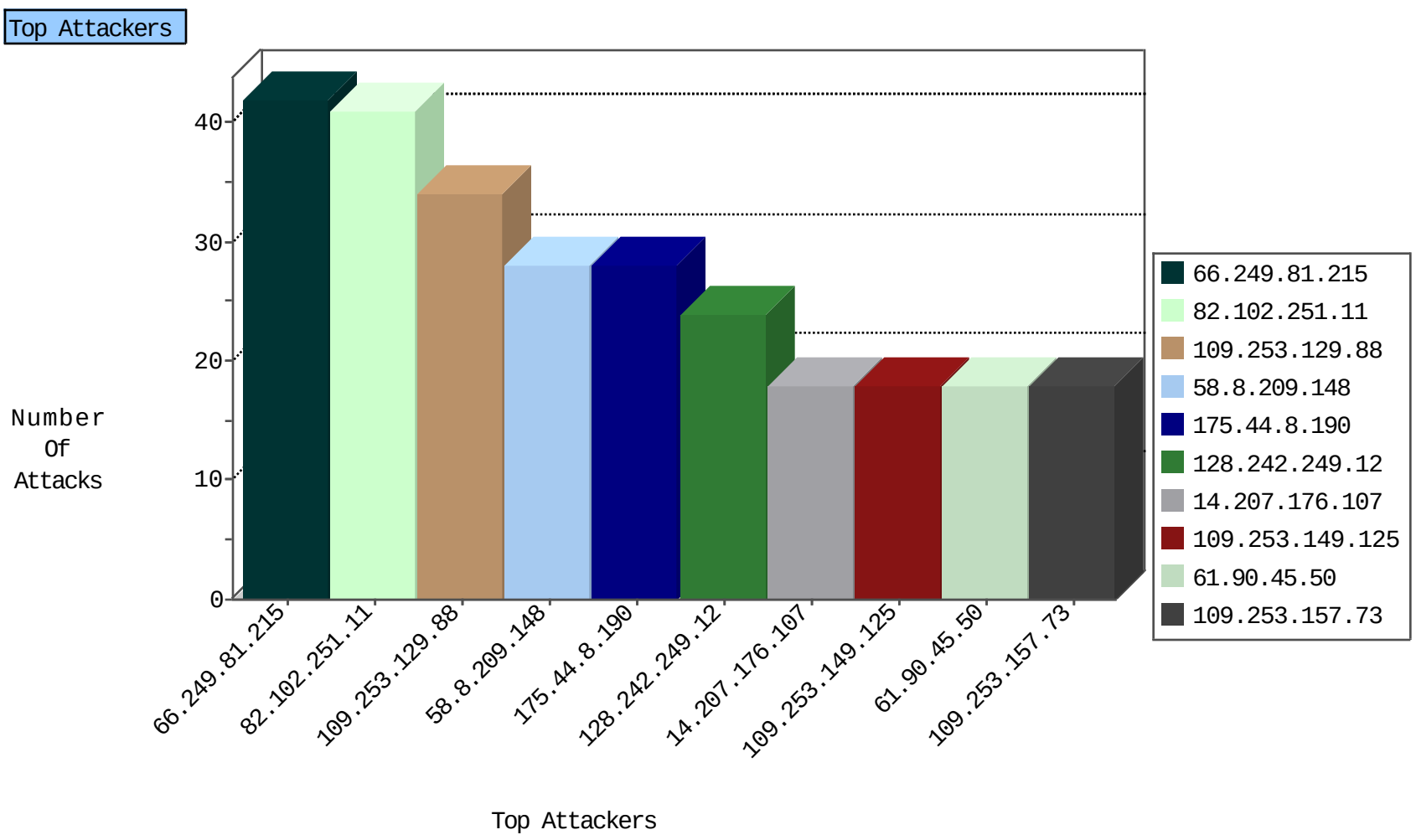
03-27-2015-22:03:07 to 03-27-2015-23:03:07

IDF Under Attack
03-27-2015-22:03:07

Top Targets



Top Attackers



03-27-2015-22:03:07 to 03-27-2015-23:03:07

Top Attackers In DDoS-Defence

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

03-27-2015-22:03:07 to 03-27-2015-23:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	24
212.34.12.150	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.19.85.22	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
37.142.182.226	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
41.97.37.118	Algeria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
175.44.8.190	China	147.237.77.74	law.idf.il	C076: HTTP: Access to - action=... (General)	Block	1
85.250.149.190	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.104.215.125	Germany	147.237.77.216	dover.idf.il	14189: HTTP: Misspelled Mozilla User-Agent (Mozila)	Block	1
46.19.85.11	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1

03-27-2015-22:03:07 to 03-27-2015-23:03:07

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	16
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
109.186.5.160	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.177.102.67	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.65	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
24.247.231.250	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.77.79.43	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.65	China	147.237.0.35	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.181.73.92	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

03-27-2015-22:03:07 to 03-27-2015-23:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
82.102.251.11	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.253.129.88	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
58.8.209.148	Thailand	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
109.253.149.125	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
14.207.176.107	Thailand	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.157.73	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
61.90.45.50	Thailand	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.81.212	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
61.90.43.76	Thailand	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
58.11.67.180	Thailand	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	7
176.12.138.163	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.143.177	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.81.218	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
61.90.43.76	Thailand	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
61.90.45.50	Thailand	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
94.230.86.238	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
58.8.209.148	Thailand	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
94.230.86.139	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
94.230.86.139	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
109.67.151.86	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	3
46.117.123.184	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
46.19.85.53	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.11	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
37.142.182.226	Israel	147.237.77.226	www.chamatz.aka.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	2
46.19.86.237	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
58.8.209.148	Thailand	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
66.249.79.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
61.90.45.50	Thailand	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.121.229.157	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
84.109.211.8	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
66.249.81.199	United States	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
46.19.86.152	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.11	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
79.180.12.186	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
5.102.254.95	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
46.121.229.157	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.56	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
84.111.111.20	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
37.46.39.195	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.205	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
5.102.254.95	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.210.209.223	Israel	147.237.77.74	law.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.7	United States	147.237.76.198	e.yohalan.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.85.128	Israel	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	1
89.138.67.117	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
46.19.85.32	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
84.109.145.156	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
175.44.8.190	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 175.44.8.190	Block	15
175.44.8.190	China	147.237.77.74	law.idf.il	PHP Attempt	Block	11
85.64.0.107	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 85.64.0.107	Block	10
37.142.182.226	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 37.142.182.226	Block	6
82.102.251.11	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 82.102.251.11	Block	5
84.228.188.177	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 84.228.188.177	Block	3
188.165.15.148	France	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
213.57.46.207	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	2
84.108.108.223	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.46.13.138	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 207.46.13.138	Block	2
84.228.188.177	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
66.249.79.96	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
207.46.13.138	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
37.142.182.226	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	1
95.233.224.172	Italy	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.30	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
54.167.175.216	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/jenin/site/english/main_index.stm	Block	1
2.54.153.183	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	1
157.55.39.187	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	1
46.19.85.137	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.66.12.93	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/faqselection.aspx	None	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.65.150	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/contactus/contactus.aspx	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/born7.stm	Block	1
85.64.0.107	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
77.1.241.26	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arafat/terrorism/english/main_index.stm	Block	1
46.117.251.79	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
157.55.39.6	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/march/24.stm	Block	1
84.228.4.173	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0212-1.stm	Block	1
66.249.73.227	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
37.26.147.194	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
87.68.214.162	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.127.182.60	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
207.46.13.16	United States	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on nakhal.idf.il//page.asp	Block	1
46.121.229.157	Israel	147.237.72.166	aka.idf.il	Unknown Parameter captcha in aka.idf.il/main/giyus/authenticationservice.asmx/authenticate	None	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.79.74	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	1
175.44.8.190	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/sip_storage/	Block	1
87.69.207.49	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.181.136.226	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
207.46.13.30	United States	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on nakhal.idf.il//page.asp	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
157.55.39.186	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1