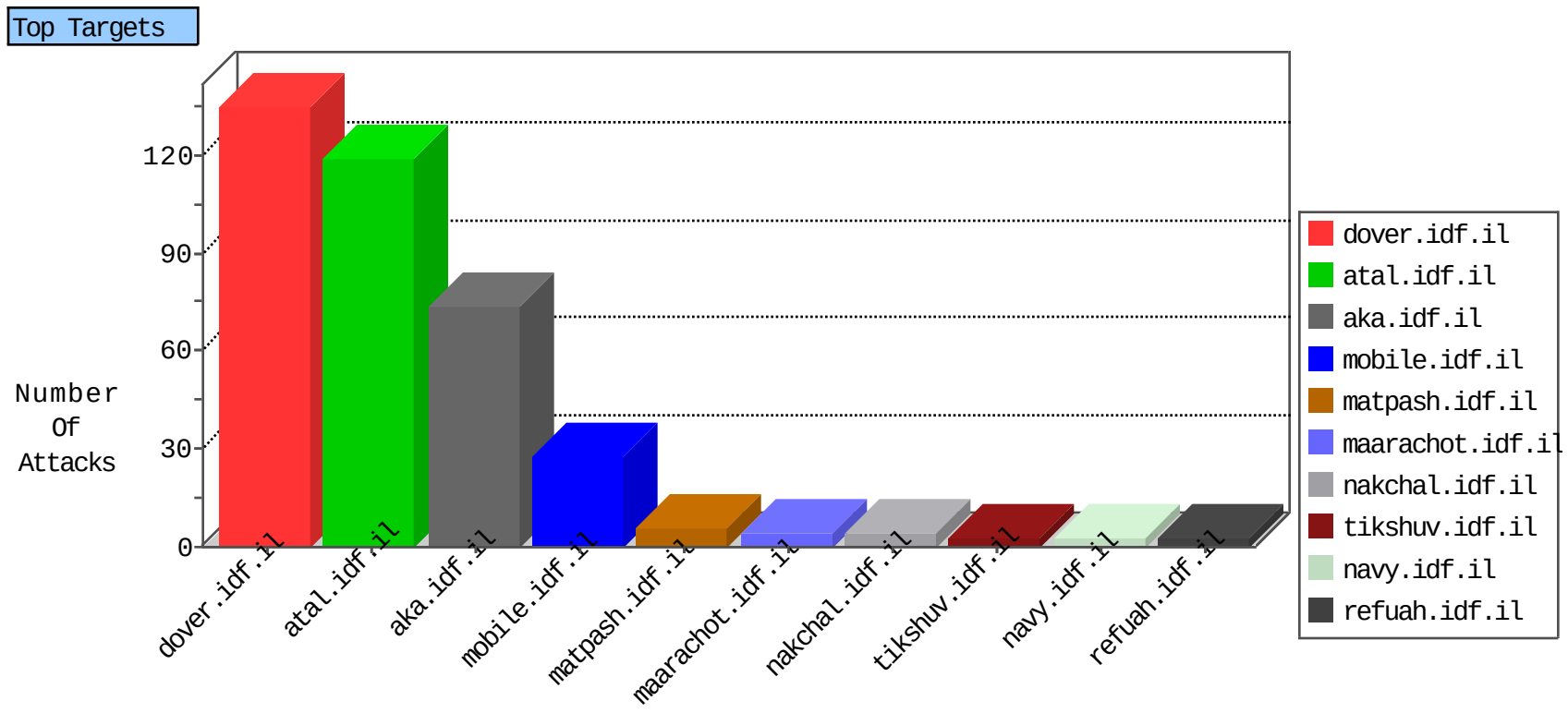
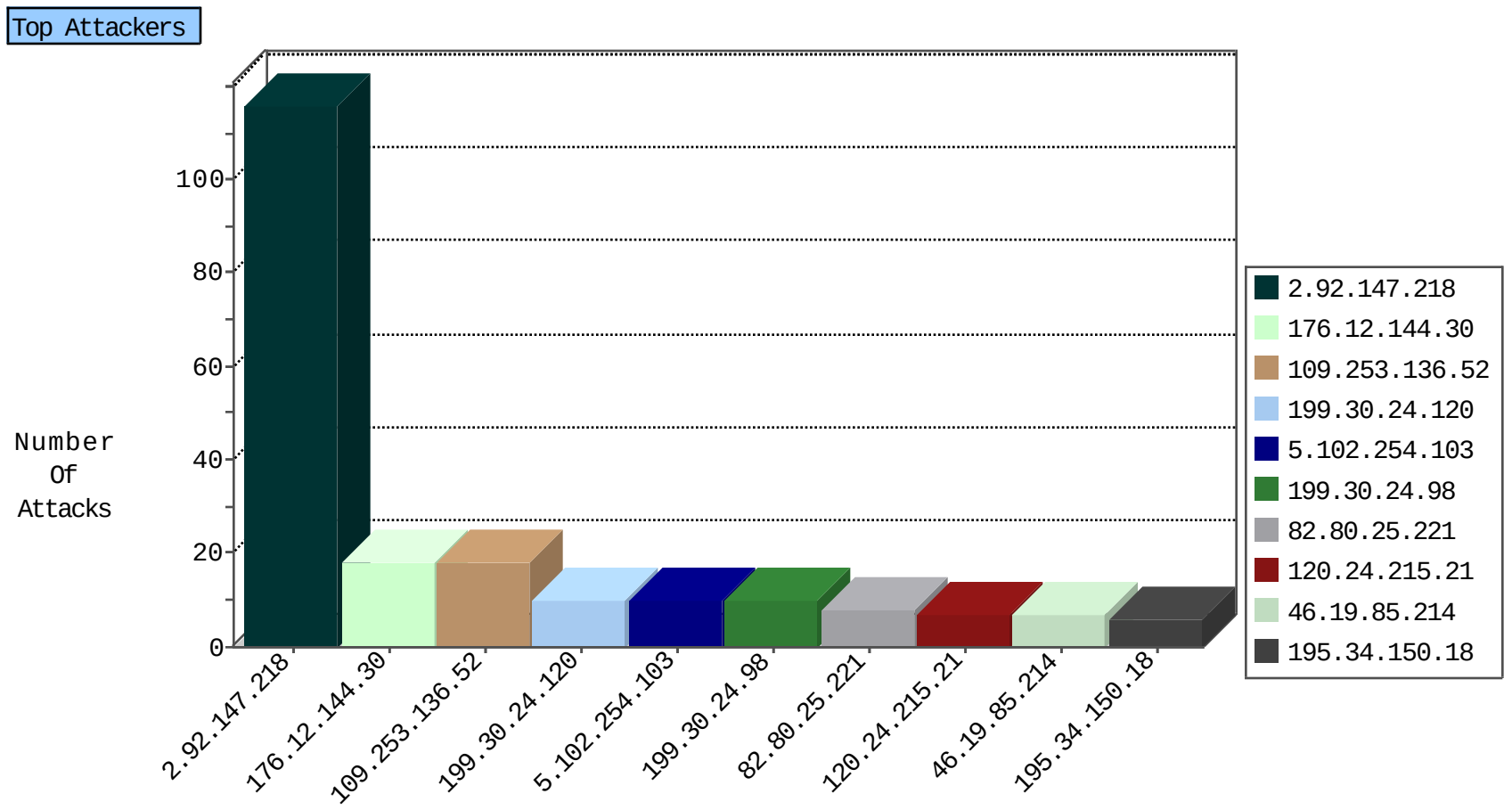
03-28-2015-12:03:00 to 03-28-2015-13:03:00

IDF Under Attack
03-28-2015-12:03:00

Top Targets



Top Attackers



03-28-2015-12:03:00 to 03-28-2015-13:03:00

Top Attackers In DDoS-Defence

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

03-28-2015-12:03:00 to 03-28-2015-13:03:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
218.186.83.101	Singapore	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
212.253.107.198	Turkey	147.237.77.74	law.idf.il	12373: HTTP: WordPress admin Login	Block	3
212.253.107.198	Turkey	147.237.77.176	matpash.idf.il	12373: HTTP: WordPress admin Login	Block	3
85.25.43.94	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.101	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	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
77.127.220.98	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
85.25.43.94	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1

03-28-2015-12:03:00 to 03-28-2015-13:03:00

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
176.228.202.39	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
120.24.215.21	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
109.253.130.214	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.67	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
211.138.34.58	China	147.237.77.243	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
5.236.218.240	Iran, Islamic Republic of	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
183.136.216.7	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
5.236.218.240	Iran, Islamic Republic of	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
120.24.215.21	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
120.24.215.21	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
120.24.215.21	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
120.24.215.21	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	ET DROP Dshield Block Listed Source	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
193.107.17.72	Russian Federation	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
5.236.218.240	Iran, Islamic Republic of	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
120.24.215.21	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
120.24.215.21	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1

03-28-2015-12:03:00 to 03-28-2015-13:03:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.92.147.218	Russian Federation	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	116
176.12.144.30	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.136.52	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
199.30.24.98	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
5.102.254.103	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	10
199.30.24.120	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
176.12.140.69	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.86.84	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
188.120.148.153	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
5.28.157.52	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
79.181.28.248	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
176.12.148.43	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
109.253.134.230	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
46.19.86.87	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
188.120.148.129	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
46.19.85.214	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
93.173.172.226	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
5.22.130.228	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
109.253.142.32	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
46.19.85.167	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
109.253.132.224	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
66.249.75.21	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
79.177.169.112	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	2
5.102.254.194	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
207.241.237.223	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.85.120	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
79.181.28.248	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
197.37.155.109	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.86.69	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.174	United States	147.237.8.14	e.orchot.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
94.230.86.156	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.117.197.209	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
188.138.17.205	France	147.237.72.217	e.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.85.214	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
141.212.122.200	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.96	United States	147.237.72.217	e.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.86.74	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
37.26.147.237	Israel	147.237.76.31	nakchal.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
141.212.122.176	United States	147.237.76.200	eitan.aka.idf.il		drop	drop	1
2.54.10.113	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
188.165.15.196	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.85.214	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.200	United States	147.237.76.44	e.refuah.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.170	United States	147.237.76.34	yohalan.idf.il		drop	drop	1
85.65.35.23	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
184.105.139.67	United States	147.237.77.234	halag.idf.il	SAM rule	drop	drop	1
37.26.147.237	Israel	147.237.76.31	nakchal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.178	United States	147.237.76.34	yohalan.idf.il		drop	drop	1
2.54.10.113	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1

03-28-2015-12:03:00 to 03-28-2015-13:03:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.33.156	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	3
207.46.13.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.112	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
77.127.90.19	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	2
66.249.75.34	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.75.34	Block	2
66.249.73.193	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	2
83.244.127.22	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
68.180.228.175	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
188.165.15.176	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9745-he/refuah.aspx	Block	1
66.249.73.201	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	1
157.55.39.41	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
87.68.60.245	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 87.68.60.245	Block	1
46.19.85.167	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
202.112.50.77	China	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 202.112.50.77	Block	1
79.177.159.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/payslips.aspx	None	1
157.55.39.153	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/announcements/2002/october/13.stm	Block	1
66.249.79.59	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1116-he/nakhal.aspx	Block	1
54.163.158.99	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
109.186.188.102	Israel	147.237.72.166	aka.idf.il	Unknown Parameter captcha in www.aka.idf.il/main/giyus/authenticationservice.asmx/authenticate	None	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/siua.stm	Block	1
84.228.230.157	Bulgaria	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	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
66.249.73.212	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/arabic/pages/default.aspx	Block	1
87.68.72.214	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
46.19.85.187	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Unknown HTTP Request Method quit in URL	Block	1
79.177.169.112	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
176.12.141.235	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.153	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/general/general.aspx	Block	1
54.163.158.99	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
109.253.135.192	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.64.171.96	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
216.218.206.67	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	Block	1
77.125.209.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
192.116.52.170	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	1
157.55.39.130	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
66.249.75.21	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.69.194.160	Israel	147.237.72.166	aka.idf.il	Unknown Parameter captcha in aka.idf.il/main/giyus/authenticationservice.asmx/authenticate	None	1
46.120.163.186	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
202.181.99.22	Japan	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/old/wp-admin/	Block	1
79.182.105.194	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/kkkkkkk=eb6a7450kkkkkkk_eb6a7450	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
66.249.65.188	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18485-he/dover.aspx	Block	1
109.253.142.32	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.228.85	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 85.250.228.85	Block	1
2.54.40.235	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Malformed URL	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1

03-28-2015-12:03:00 to 03-28-2015-13:03:00