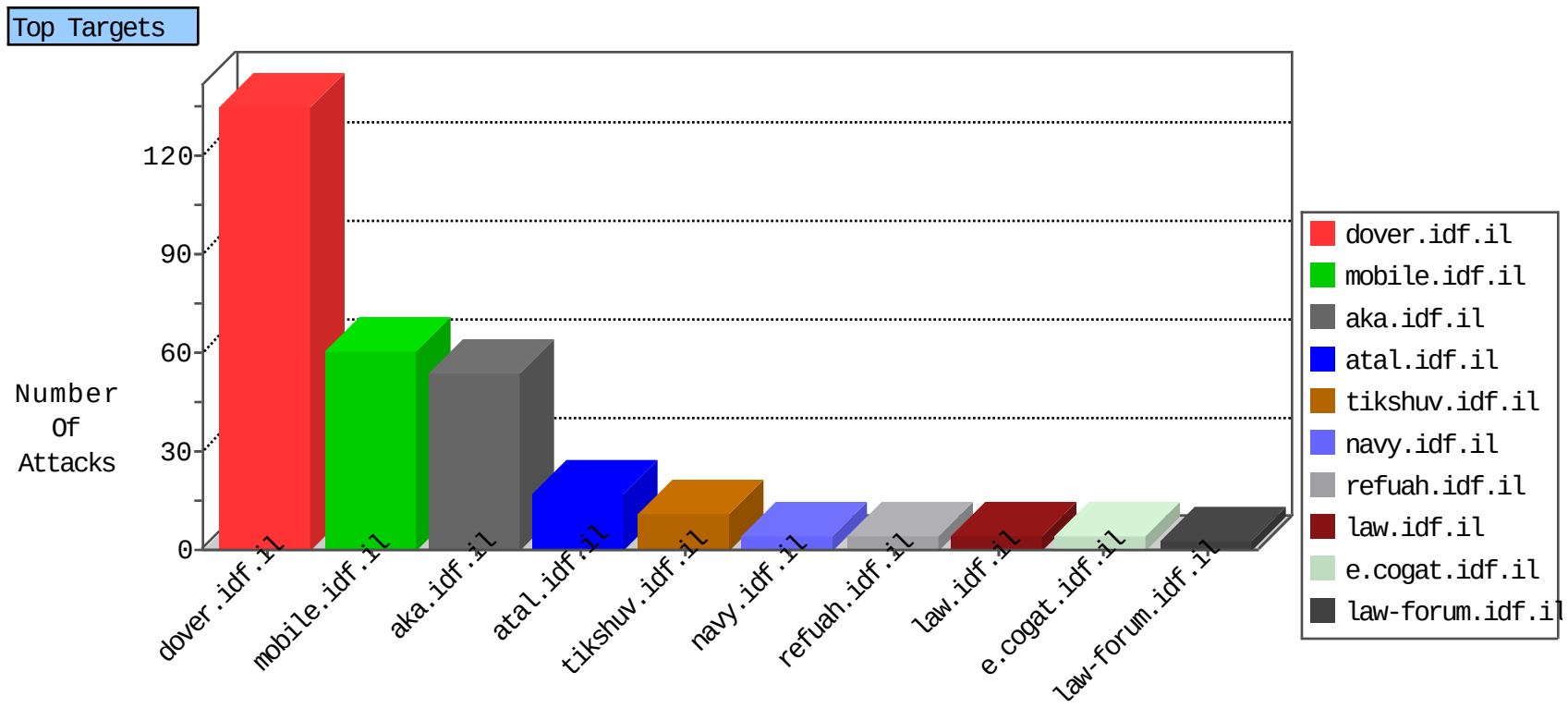
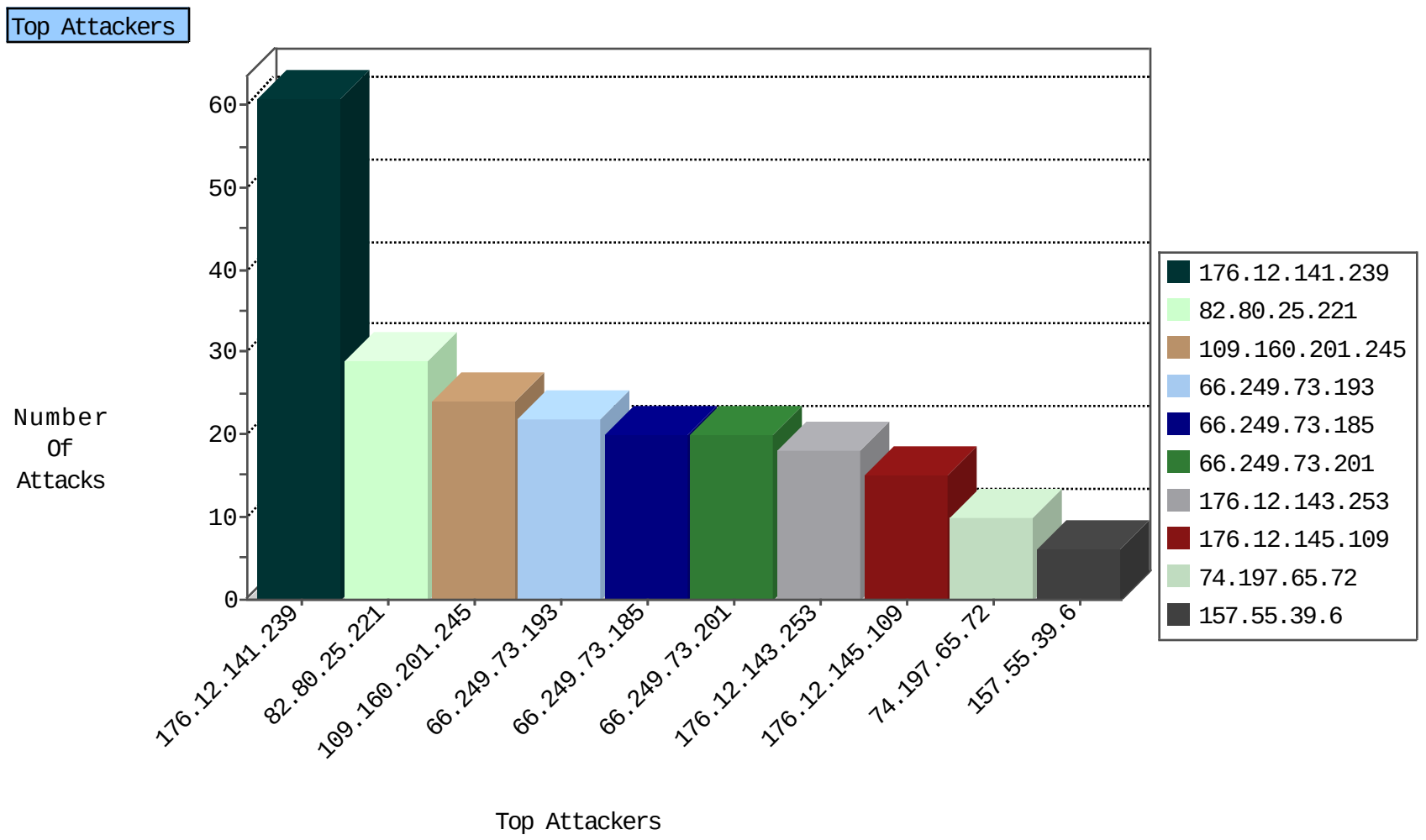
03-28-2015-09:03:00 to 03-28-2015-10:03:00

IDF Under Attack
03-28-2015-09:03:00

Top Targets



Top Attackers



03-28-2015-09:03:00 to 03-28-2015-10:03:00

Top Attackers In DDoS-Defence

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

03-28-2015-09:03:00 to 03-28-2015-10:03:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count

03-28-2015-09:03:00 to 03-28-2015-10:03:00

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	29
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
93.172.163.56	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.108.110.139	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.79.22	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
89.139.41.21	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
81.252.125.133	France	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
74.197.65.72	United States	147.237.77.74	law.idf.il	SERVER-WEBAPP bad HTTP/1.1 request, Potentially worm attack	1
61.240.144.66	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
95.226.216.150	Italy	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
81.252.125.133	France	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
74.197.65.72	United States	147.237.77.19	law-forum.idf.il	SERVER-WEBAPP bad HTTP/1.1 request, Potentially worm attack	1
66.249.69.122	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
58.20.54.249	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
95.226.216.150	Italy	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 3072	1

03-28-2015-09:03:00 to 03-28-2015-10:03:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
176.12.141.239	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	60
66.249.73.193	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
66.249.73.185	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.143.253	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.160.201.245	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	16
176.12.145.109	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.73.201	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.160.201.245	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8
157.55.39.6	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
68.180.228.232	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
74.197.65.72	United States	147.237.77.61	e.cogat.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
46.19.85.35	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
54.174.17.106	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.85.93	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
80.246.133.50	Israel	147.237.0.34	tikshuv.idf.il	Web Servers Slow HTTP Denial of Service	Web Server Enforcement Violation	reject	2
46.19.85.179	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
80.246.133.147	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
141.212.122.89	United States	147.237.77.121	e.navy.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
176.12.141.239	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
89.139.41.21	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.197	United States	147.237.77.121	e.navy.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.200	United States	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.205	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.86.152	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.83	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	1
84.109.64.236	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.161	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
188.120.148.188	Israel	147.237.72.167	ishurim.aka.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
46.116.191.223	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
176.12.145.109	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
80.246.133.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	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
74.197.65.72	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 74.197.65.72	Block	1
192.114.23.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	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
176.12.146.81	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.185	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/homefront/homefront3.stm	Block	1
31.172.201.231	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/brothers/faq/default.asp	None	1
188.165.15.176	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/templates/shared/usercontrols/headerupper/	Block	1
125.24.31.221	Thailand	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/brothers/printpreview/default.asp	None	1
74.197.65.72	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
207.46.13.16	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ie-welcome.stm	Block	1
62.210.114.129	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/8/3198.pdf/trackback/	Block	1
176.12.147.40	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.64.9.249	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$txtOther in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.85.125	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
176.12.142.41	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.125.132.23	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
207.46.13.43	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
66.249.69.36	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
176.12.147.204	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
85.64.84.15	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/viewpniot.aspx	None	1
74.197.65.72	United States	147.237.77.19	law-forum.idf.il	Multiple Unauthorized URL Access from 74.197.65.72	Block	1
46.19.85.205	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	1
176.12.142.218	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.105.8.166	Russian Federation	147.237.72.166	aka.idf.il	Unknown HTTP Request Method COOK in URL www.aka.idf.il/brothers/skira/default.asp	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
66.249.69.122	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
176.12.149.144	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
101.226.168.212	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
74.197.65.72	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
188.165.15.231	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/638.pdf	Block	1
79.182.127.18	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/terms.aspx	None	1
66.249.73.185	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	1
5.29.86.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.43.25.178	Turkey	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/brothers/skira/default.asp	None	1
122.154.45.10	Thailand	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/brothers/klali/default.asp	None	1