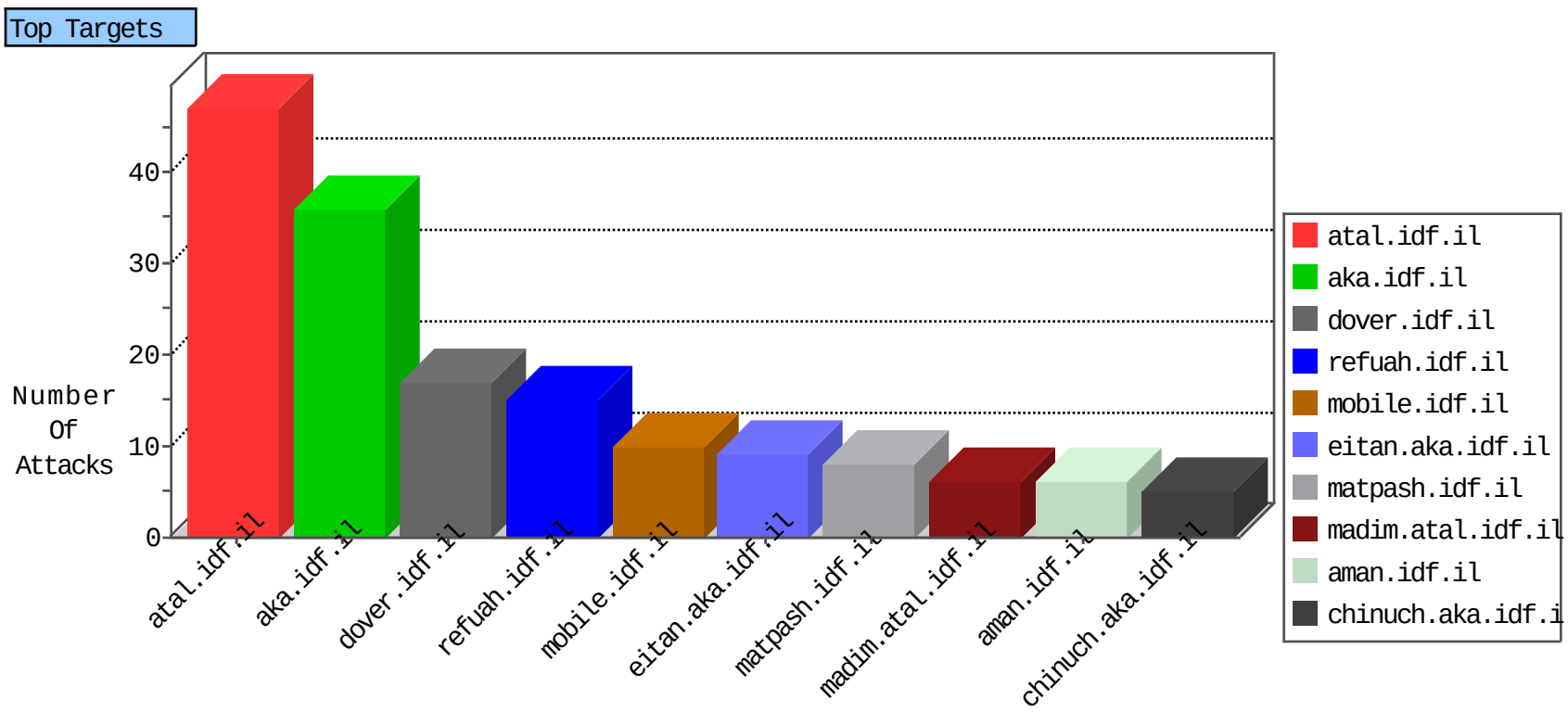
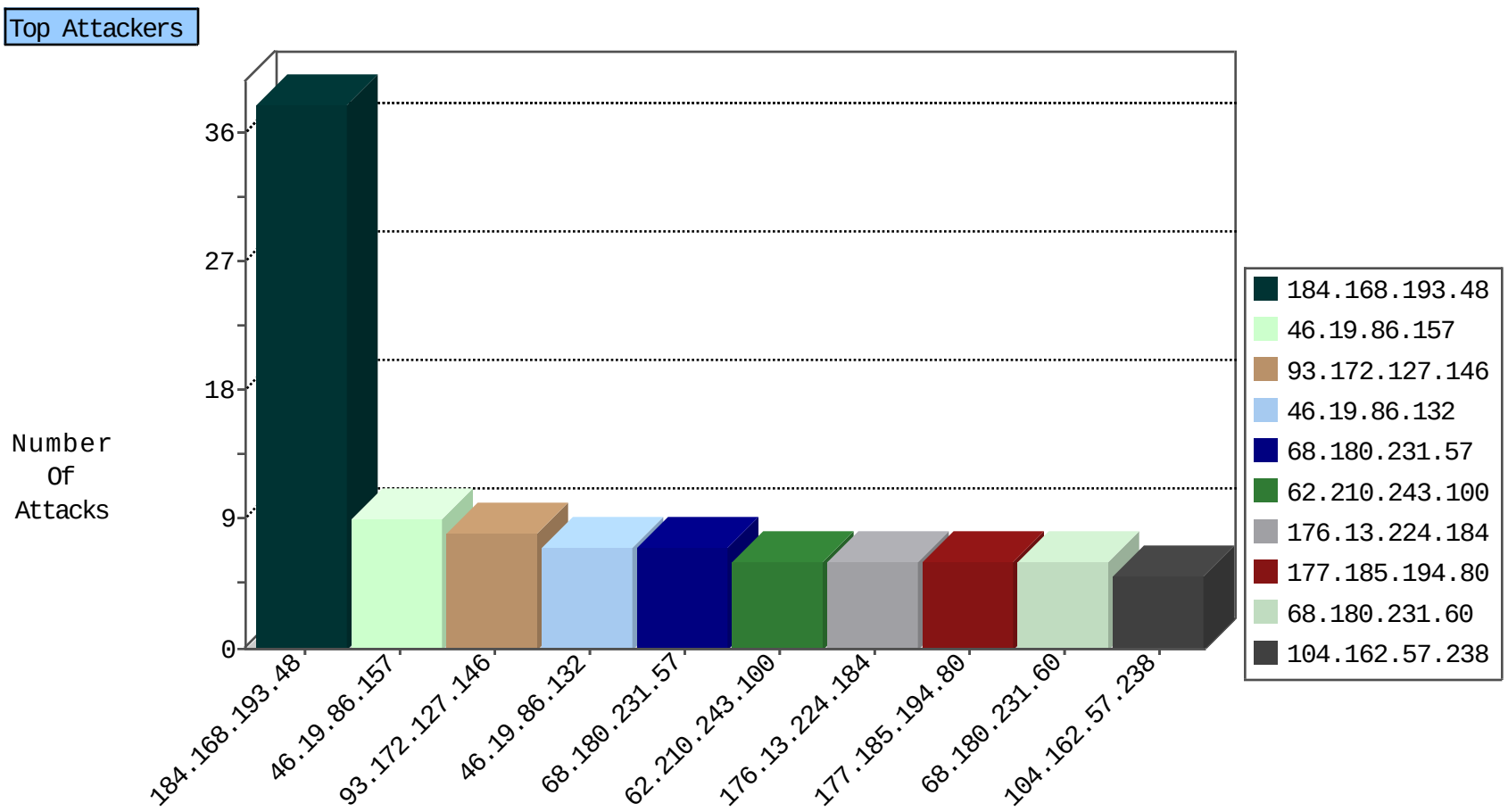
09-29-2016-04:04:07 to 09-29-2016-05:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-29-2016-04:04:07 to 09-29-2016-05:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.174.94.235	Netherlands	147.237.76.196	e.sviva.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.197	e.himush.idf.il	Black List	drop	1

09-29-2016-04:04:07 to 09-29-2016-05:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.168.193.48	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
184.168.193.48	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.193.48	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
177.185.194.80	Brazil	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3

09-29-2016-04:04:07 to 09-29-2016-05:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
184.168.193.48	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	20
177.185.194.80	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	3
5.255.90.133	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.72.14	Cote D'Ivoire	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
104.160.176.212	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
74.82.47.18	147.237.77.216	United States	dover.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1
62.210.243.100	147.237.0.19	France	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
40.121.139.43	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
40.121.139.43	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
14.169.54.252	147.237.76.176	Vietnam	test.ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
196.47.173.21	147.237.72.14	Cote D'Ivoire	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
104.160.176.212	147.237.76.39	United States	mobile.meitav.idf.i	ET SCAN NMAP -sS window 3072	1
74.82.47.41	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potentia Scan or Infection	1
66.249.64.68	147.237.72.156	United States	aman.idf.il	WEB-CGI redirect access	1
58.220.2.5	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
40.121.139.43	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
40.121.139.43	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.72.14	Cote D'Ivoire	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1

09-29-2016-04:04:07 to 09-29-2016-05:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
93.172.127.146	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.132	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.157	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
176.13.224.184	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
104.162.57.238	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.32	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.79.86.129	Netherlands	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
157.55.39.83	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.124	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.203.181	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
68.180.231.57	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.174	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.55.9.149	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
12.11.109.225	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
31.210.188.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
68.180.231.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.180.231.60	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
217.55.207.50	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.157	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
74.82.47.43	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.37	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.255.90.133	Netherlands	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
99.133.156.239	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
62.210.243.100	France	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.208	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
173.61.38.115	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.53	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
216.218.206.74	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
62.210.243.100	France	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.139.83	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
184.105.247.223	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.13.17.204	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
79.177.8.165	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
216.218.206.104	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
62.210.243.100	France	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.139.120	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.13	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
188.120.154.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.157	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
5.102.253.115	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
84.229.13.42	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
62.210.243.100	France	147.237.0.33	idf.il	drop		drop	1
184.105.247.208	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.32	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.205.111	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

09-29-2016-04:04:07 to 09-29-2016-05:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.137.105	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
84.94.48.88	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/viewpayslip.a	Block	2
66.249.64.68	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/redirects/ssl-redirect.html	Block	1
180.97.106.161	China	147.237.76.147	chinuch.aka.idf.il	Multiple NULL Character in Method from 180.97.106.161	Block	1
46.19.86.132	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
216.7.150.84	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/inner.asp	Block	1
180.97.106.37	China	147.237.72.167	ishurim.aka.idf.il	Distributed NULL Character in Method	Block	1
66.249.64.134	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding aI_;fAQ&e>{GbP6@ywx@zx!d/u58^O/QN){GDx1akZ.v{MDZ42FdE_vwL-@_o)3ii;1 in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
180.97.106.162	China	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
84.229.13.42	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
46.117.117.24	Israel	147.237.72.166	aka.idf.il	Unknown Parameter asm in www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	None	1
180.97.106.161	China	147.237.76.39	mobile.meitav.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8818-he/refuah.aspx	Block	1
180.97.106.162	China	147.237.77.176	matpash.idf.il	Distributed NULL Character in Method	Block	1
96.250.215.27	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
180.97.106.161	China	147.237.76.39	mobile.meitav.idf.il	Distributed NULL Character in Method	Block	1
66.249.76.32	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/iturim/asp/displayallsoldiers.asp	Block	1
204.79.180.16	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
157.55.39.36	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/page.asp	Block	1
66.249.64.60	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/iturim/asp/displayallsoldiers.asp	Block	1
180.97.106.161	China	147.237.76.147	chinuch.aka.idf.il	Multiple Illegal Byte Code Character in Method from 180.97.106.161	Block	1
207.46.13.6	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
180.97.106.37	China	147.237.72.167	ishurim.aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	1

09-29-2016-04:04:07 to 09-29-2016-05:04:07