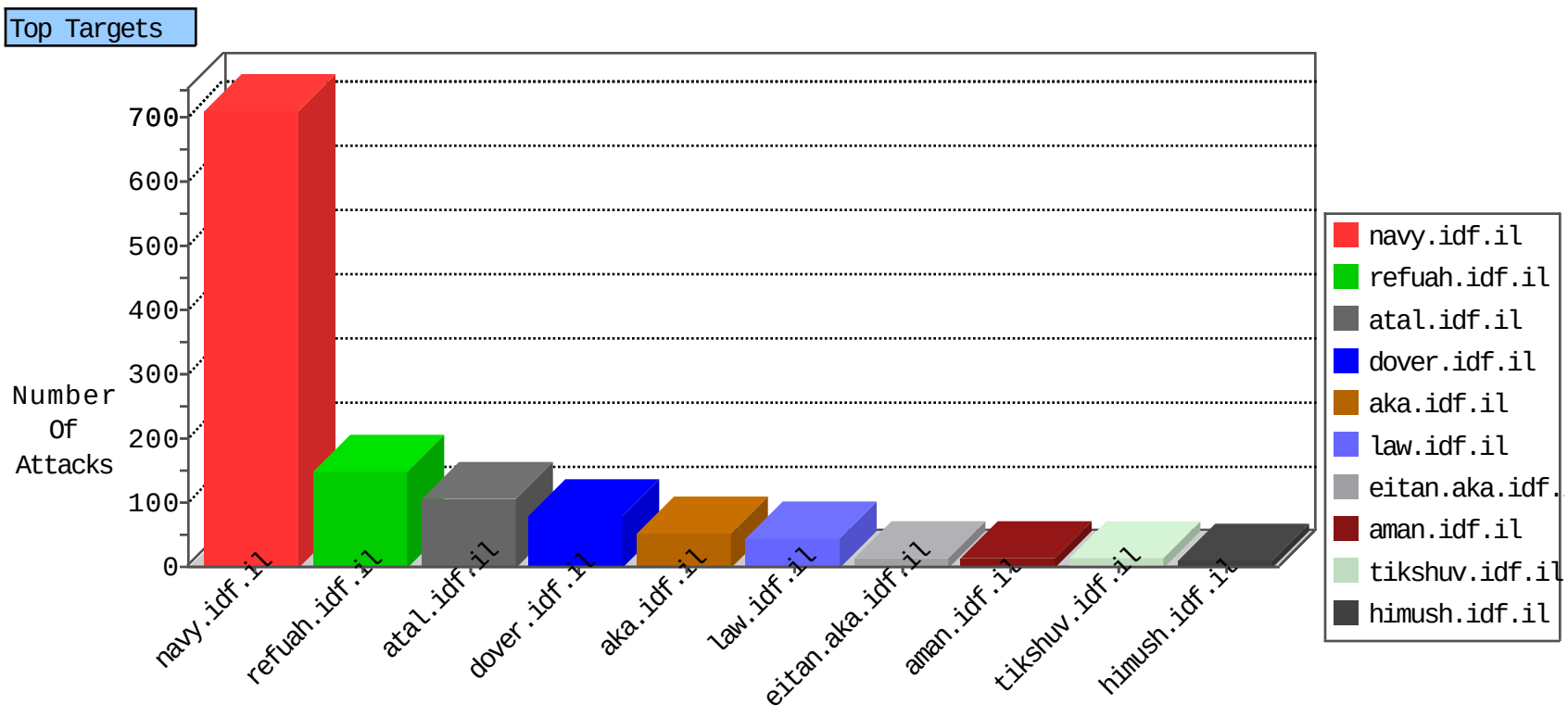
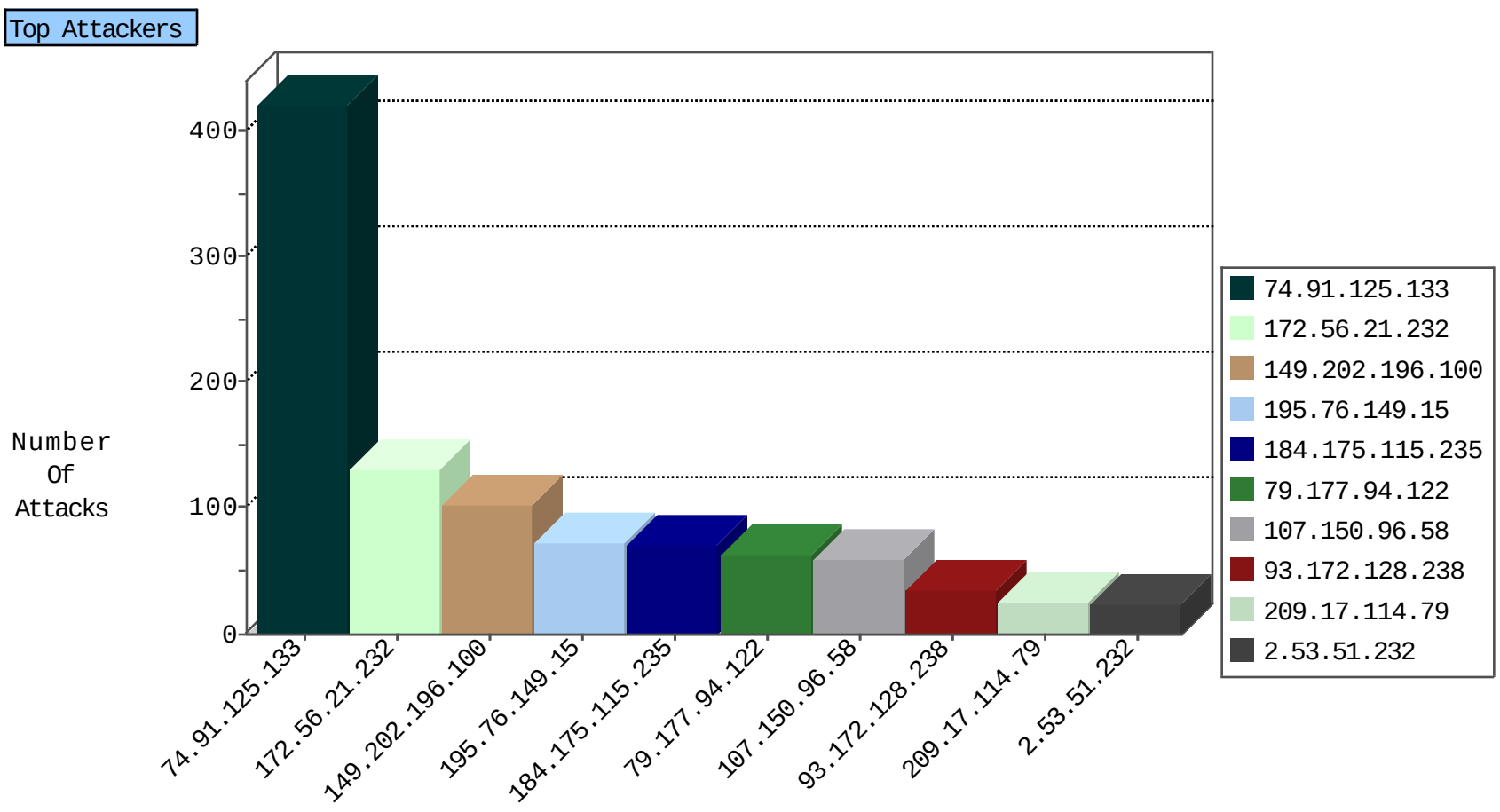
09-10-2016-00:04:02 to 09-10-2016-01:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-10-2016-00:04:02 to 09-10-2016-01:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
98.139.135.129	United States	147.237.76.201	e.atal.idf.il	Invalid TCP Flags	drop	1
185.94.111.1	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

09-10-2016-00:04:02 to 09-10-2016-01:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.76.149.15	Spain	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
209.17.114.79	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	11
207.178.197.44	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
187.61.50.197	Brazil	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
195.76.149.15	Spain	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
46.165.197.142	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
108.166.190.139	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
203.146.140.196	Thailand	147.237.76.147	chinuch.aka.idf.i	34161: ICMP: Communication with Destination Host is Administratively Prohibited (Code 10)	Block	1
209.17.114.79	United States	147.237.77.74	law.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

09-10-2016-00:04:02 to 09-10-2016-01:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.76.149.15	147.237.76.42	Spain	refuah.idf.il	SQL Injection - Select From	54
187.61.50.197	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	18
209.17.114.79	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
207.178.197.44	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
91.121.132.153	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
202.112.38.190	147.237.72.167	China	ishurim.aka.idf.il	GPL SCAN nmap TCP	2
187.19.178.147	147.237.77.216	Brazil	dover.idf.il	Xenu Link Sleuth User Agent	2
93.158.203.147	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
59.72.153.2	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
46.4.63.2	147.237.77.170	Germany	maarachot.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
179.43.141.198	147.237.72.156	Switzerland	aman.idf.il	ET SCAN Potential SSH Scan	1
139.162.160.132	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.128.144.131	147.237.76.148	Canada	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.147	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
216.81.230.167	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.147	147.237.76.39	Netherlands	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
69.24.208.162	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
195.88.208.193	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN NMAP -sS window 1024	1
59.72.153.2	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
193.201.225.73	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
178.79.141.130	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
107.6.179.131	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
94.102.48.195	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1

09-10-2016-00:04:02 to 09-10-2016-01:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
74.91.125.133	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	361
172.56.21.232	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	131
149.202.196.100	France	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	99
79.177.94.122	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	61
93.172.128.238	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
168.232.169.82		147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
37.48.105.67	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
158.85.253.245	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	18
74.91.125.133	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
74.91.125.133	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	16
74.91.125.133	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	16
74.91.125.133	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.43.114.91	Palestinian Territory, Occupied	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
83.168.250.50	Sweden	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
89.146.28.138	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.174.55.11	Germany	147.237.77.233	atal.idf.il	drop	SAM rule	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
107.150.96.58	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.116	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.51.232	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
107.150.96.58	China	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
184.175.115.235	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
107.150.96.58	China	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
184.175.115.235	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.53.51.232	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
184.175.115.235	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
107.150.96.58	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.53.51.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
107.150.96.58	China	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.53.51.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
184.175.115.235	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
107.150.96.58	China	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
80.246.130.128	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.51.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
107.150.96.58	China	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
2.53.51.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
184.175.115.235	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
107.150.96.58	China	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
37.26.149.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
81.218.183.37	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
184.175.115.235	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
184.175.115.235	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
184.175.115.235	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
184.175.115.235	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
176.13.231.212	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.140	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
184.175.115.235	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
184.175.115.235	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

09-10-2016-00:04:02 to 09-10-2016-01:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.228.204	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/givus	Block	3
66.249.66.107	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.107	Block	2
46.43.114.91	Palestinian Territory, Occupied	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/miluim/about.aspx	Block	2
79.180.218.42	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
176.13.240.98	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	1
73.75.139.2	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
37.128.98.194	Poland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/edim/library/generaldoc.asp	Block	1
81.18.213.246	Poland	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.249.66.107	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/assetlinks.json	Block	1
207.46.13.163	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-11081-he	Block	1
77.139.241.56	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
85.64.242.94	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/lomdim/bakashot/abroad/default.asp	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
79.177.94.122	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
46.43.114.91	Palestinian Territory, Occupied	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.43.114.91	Block	1
93.172.128.238	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.69.97	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	1
79.177.94.122	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
174.115.29.28	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
71.194.220.107	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1

09-10-2016-00:04:02 to 09-10-2016-01:04:02