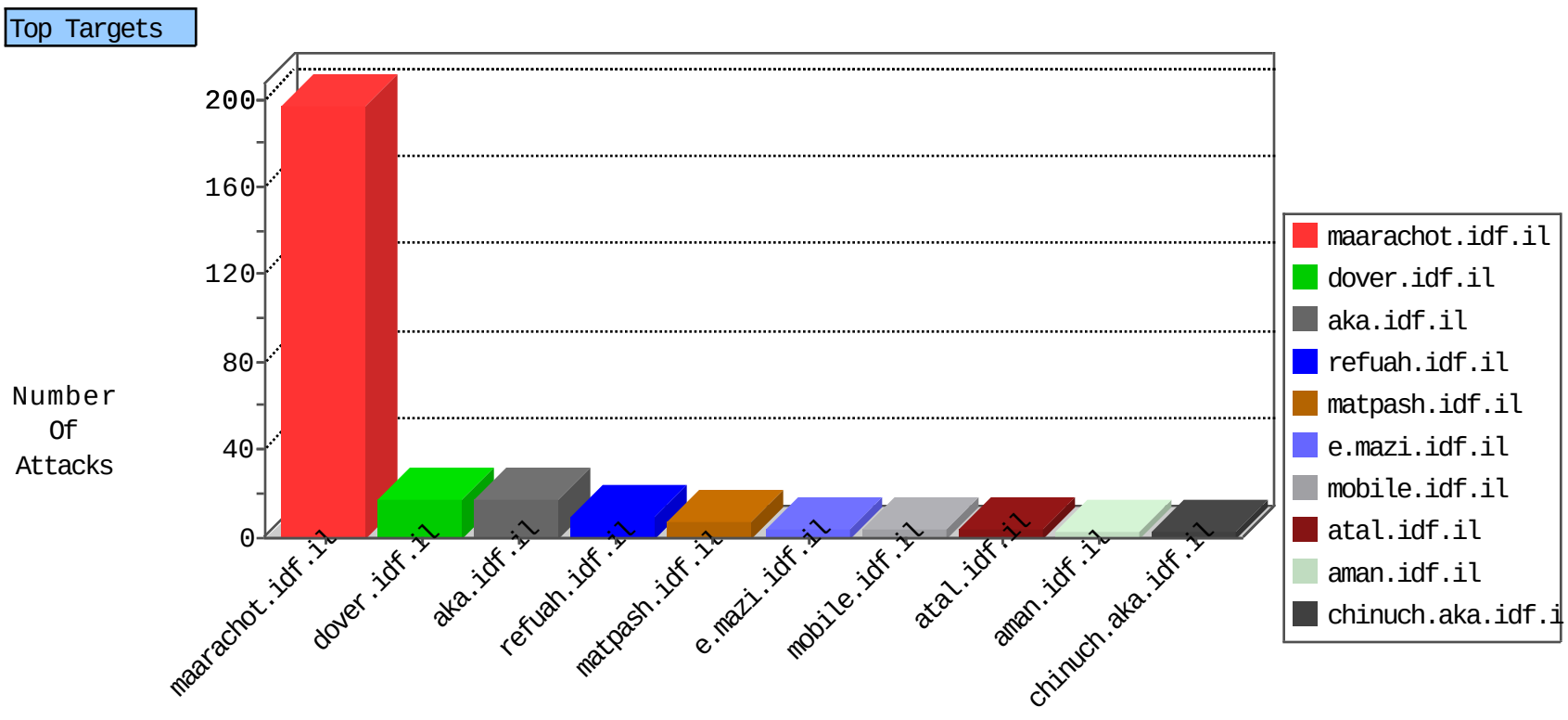
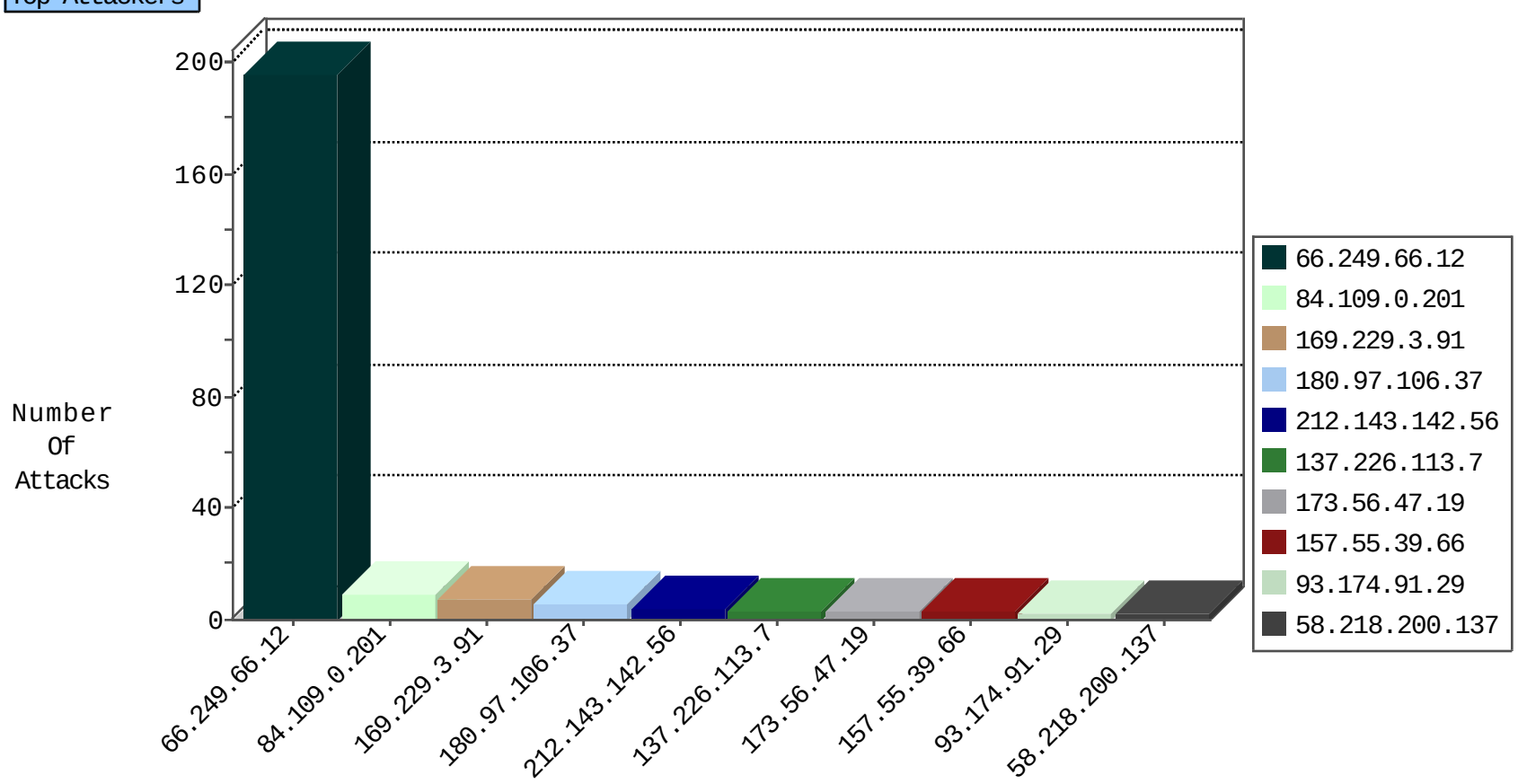
09-21-2016-03:04:02 to 09-21-2016-04:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-21-2016-03:04:02 to 09-21-2016-04:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.32.205.187	Netherlands	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
204.42.253.2	United States	147.237.76.30	himush.idf.il	Black List	drop	1
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1

09-21-2016-03:04:02 to 09-21-2016-04:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.209	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-21-2016-03:04:02 to 09-21-2016-04:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.12	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	196
66.249.66.177	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
58.218.200.137	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
212.156.129.222	147.237.77.243	Turkey	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
46.183.223.228	147.237.0.35	Latvia	akaws.idf.il	ET SCAN Potential SSH Scan	1
211.149.222.5	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
14.125.20.133	147.237.77.178	China	e.matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
128.232.110.28	147.237.76.39	United Kingdom	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
122.72.53.188	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
116.71.128.85	147.237.77.233	Pakistan	atal.idf.il	ET SCAN NMAP -sS window 1024	1
107.172.246.40	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
93.174.91.29	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
212.156.129.222	147.237.77.205	Turkey	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
31.24.228.20	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.213.241	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
125.212.234.99	147.237.77.235	Vietnam	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
118.103.126.194	147.237.76.31	Japan	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
116.71.128.85	147.237.77.226	Pakistan	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.91.29	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1

09-21-2016-03:04:02 to 09-21-2016-04:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.109.0.201	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
173.56.47.19	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
84.109.0.201	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
157.55.39.66	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.109.0.201	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
93.104.215.125	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
180.97.106.37	China	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
157.55.39.161	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.131	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.253.220.165	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.161	China	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.60	United States	147.237.0.35	akaws.idf.il	drop		drop	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.164	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
137.226.113.7	Germany	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.37	China	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.102.242.32	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.132	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
137.116.71.170	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
180.97.106.162	China	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.165	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
101.199.112.45	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.37	China	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.196	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.163	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
137.116.71.170	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.0.113.241	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.37	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.166	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.128	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
106.186.113.169	Japan	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
180.97.106.37	China	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.163	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
137.226.113.7	Germany	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.109.0.201	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
180.97.106.37	China	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.129	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.253.203.155	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.161	China	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.188.72.194	Russian Federation	147.237.76.42	refuah.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	1
169.229.3.91	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.164	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
137.226.113.7	Germany	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
213.57.199.145	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-21-2016-03:04:02 to 09-21-2016-04:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/kamlar/klali/default.asp	None	1
66.249.64.108	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.64.108	Block	1
77.234.44.151	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-23074-ar/dover.aspx	Block	1
66.249.64.112	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.64.112	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.66.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/894-he/dover.aspx	Block	1
180.76.15.140	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
66.249.92.91	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew akhal/к	Block	1
66.249.64.112	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/gdegsd.aspx	Block	1
139.162.13.205	Singapore	147.237.77.176	matpash.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/faq/faq.asp	Block	1
190.230.62.31	Argentina	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
68.180.228.27	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.64.128	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
142.165.113.48	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
46.120.113.100	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
204.79.180.253	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
66.249.64.181	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/62938.pdf	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1

09-21-2016-03:04:02 to 09-21-2016-04:04:02