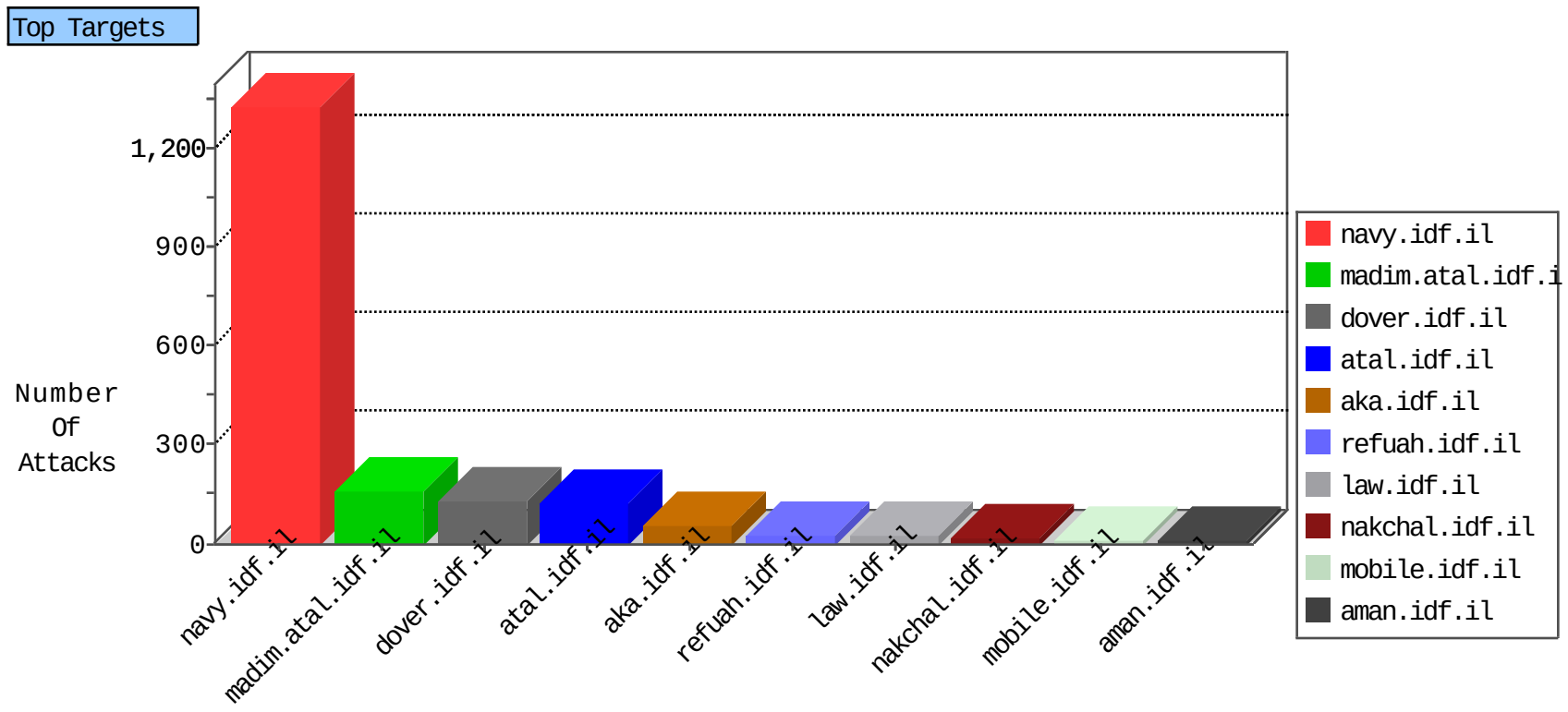
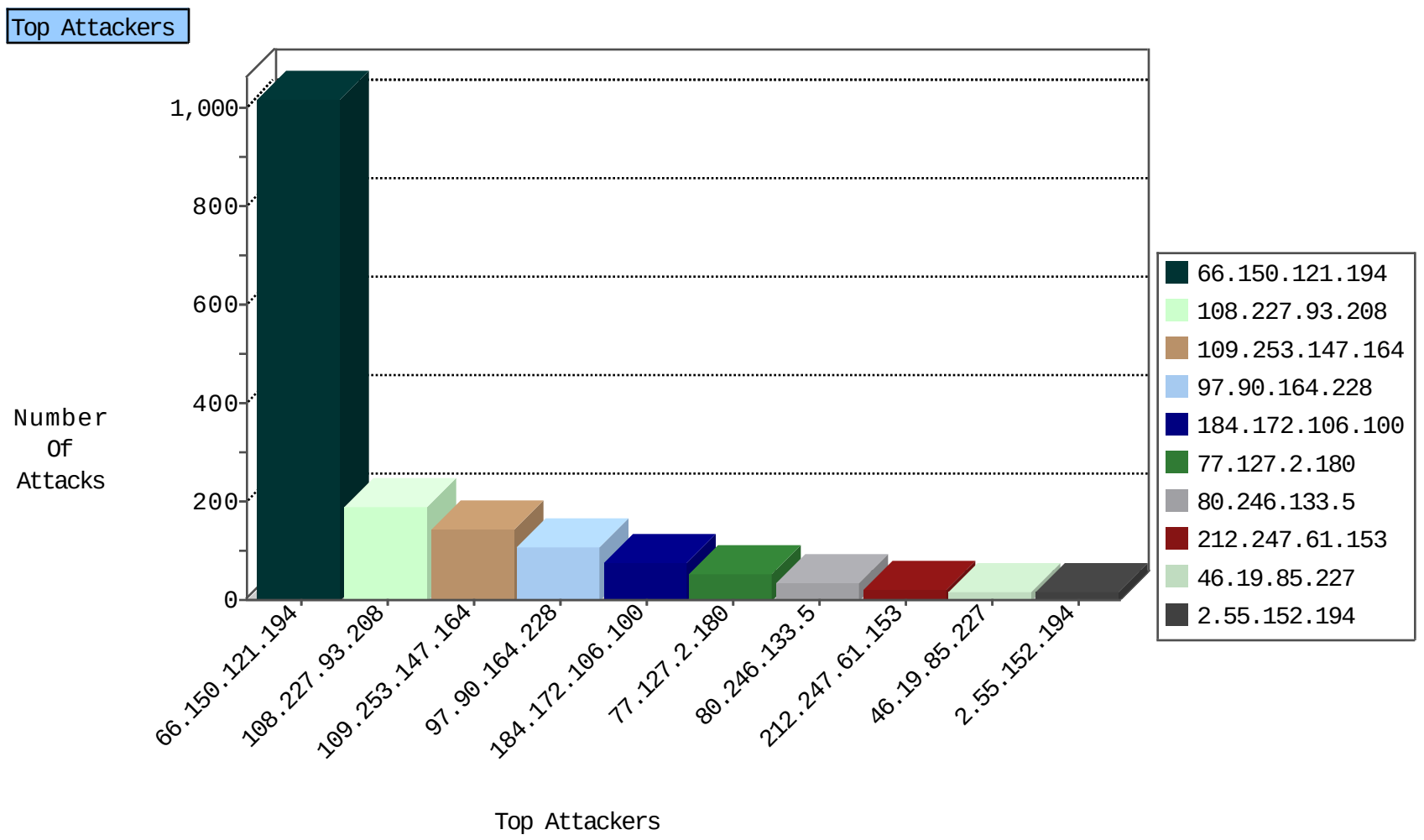
09-22-2016-07:04:08 to 09-22-2016-08:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-22-2016-07:04:08 to 09-22-2016-08:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.248.163.3	Netherlands	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
45.32.205.187	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
185.81.157.161	France	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
169.54.233.119	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	1

09-22-2016-07:04:08 to 09-22-2016-08:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.247.61.153	Sweden	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	7
184.172.106.100	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
184.172.106.100	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.172.106.100	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6

09-22-2016-07:04:08 to 09-22-2016-08:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
184.172.106.100	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	55
212.247.61.153	147.237.77.74	Sweden	law.idf.il	SQL Injection - Select From	14
118.103.126.194	147.237.76.44	Japan	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
100.13.130.4	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.130.55	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
64.137.168.128	147.237.0.15	Canada	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
46.183.223.228	147.237.76.30	Latvia	himush.idf.il	ET SCAN Potential SSH Scan	1
206.246.150.226	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
195.70.44.28	147.237.0.19	Hungary	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.238.45	147.237.0.33	United Kingdom	idf.il	ET SCAN NMAP -sS window 1024	1
118.103.126.194	147.237.0.200	Japan	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
85.17.73.11	147.237.8.27	Netherlands	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	1
80.15.154.133	147.237.0.200	France	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
46.183.223.228	147.237.77.74	Latvia	law.idf.il	ET SCAN Potential SSH Scan	1
31.24.228.20	147.237.77.121	United Kingdom	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
206.246.150.226	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1

09-22-2016-07:04:08 to 09-22-2016-08:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.150.121.194	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	995
108.227.93.208	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	188
97.90.164.228	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	107
80.246.133.5	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
66.150.121.194	United States	147.237.76.86	navy.idf.il	SYN Attack		monitor	17
77.127.2.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
77.127.2.180	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
77.127.2.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
2.55.24.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
89.138.163.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
77.127.2.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
77.127.2.180	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.86.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.147.229	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
89.139.125.84	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.85.114	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.227	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.208	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.227	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.148	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
62.0.234.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.234.148	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
2.55.10.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.169	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.40	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
80.246.130.55	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
172.58.16.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.150.121.194	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
37.46.41.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.148	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
199.203.215.1	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.201	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.201	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
80.246.130.55	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
66.150.121.194	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
2.55.10.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.174	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
82.81.222.167	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.226.161.155	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.55.10.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2

09-22-2016-07:04:08 to 09-22-2016-08:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.147.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	142
2.55.152.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
62.219.198.6	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	6
62.219.198.6	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 62.219.198.6	Block	5
2.53.138.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.138.115.145	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	3
212.25.84.200	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/templatecontrols/generic/	Block	2
2.53.30.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.130.55	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
109.253.197.206	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
66.249.76.74	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/assetlinks.json	Block	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	1
80.246.133.5	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
172.56.12.159	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/.well-known/apple-app-site-association	Block	1
2.55.136.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.31	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/brothers/skira/default.asp-catid=57478&docid	Block	1
82.81.142.140	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/sachar/scriptresource.axd	None	1
62.219.198.6	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
180.76.15.21	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17060-en/dover.aspx>.	Block	1
77.127.2.180	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
180.97.106.161	China	147.237.76.147	chinuch.aka.idf.il	Illegal Byte Code Character in Method	Block	1
40.77.167.41	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
212.199.224.24	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/images/trans.gif	Block	1
66.249.76.54	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding jzj9c^XCz2B_1;Q2&-N@ ob-P/tUX]lbvhezwj_IWc in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
180.97.106.161	China	147.237.76.147	chinuch.aka.idf.il	NULL Character in Method	Block	1

09-22-2016-07:04:08 to 09-22-2016-08:04:08