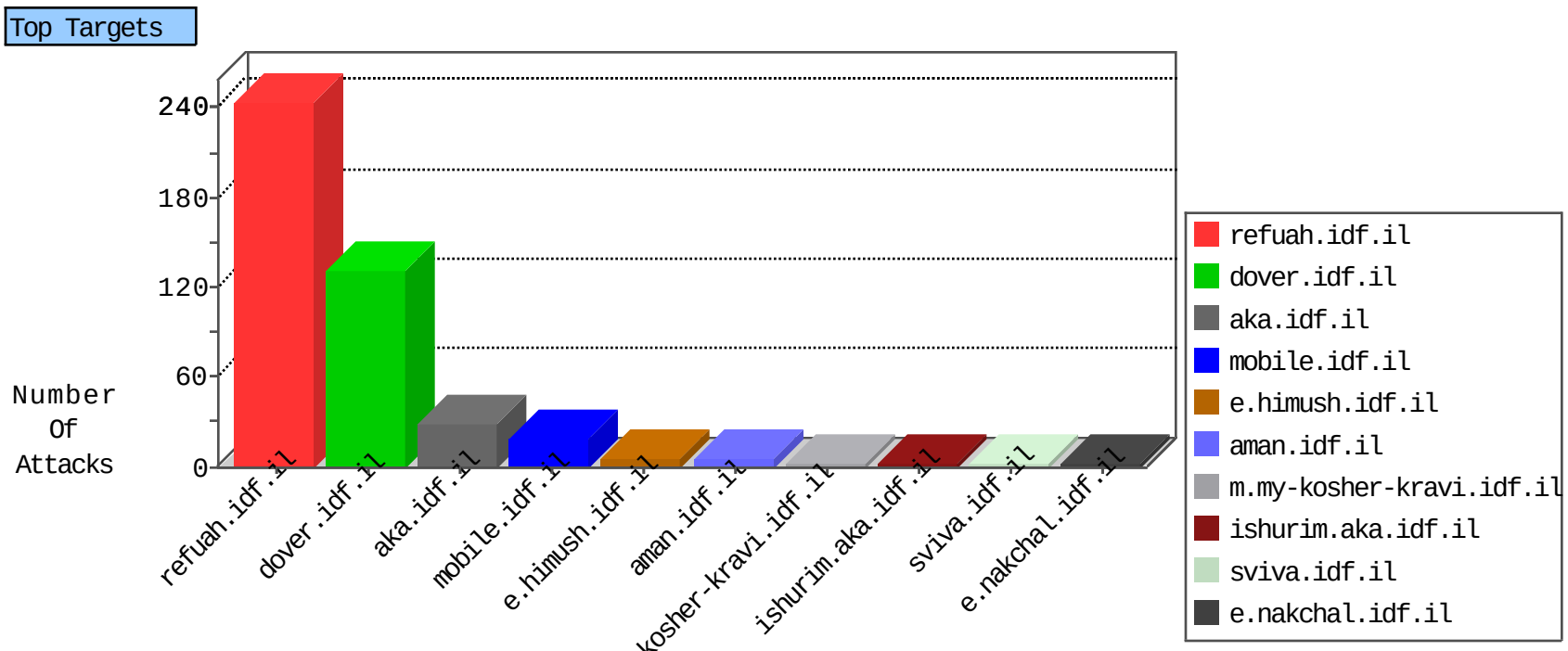
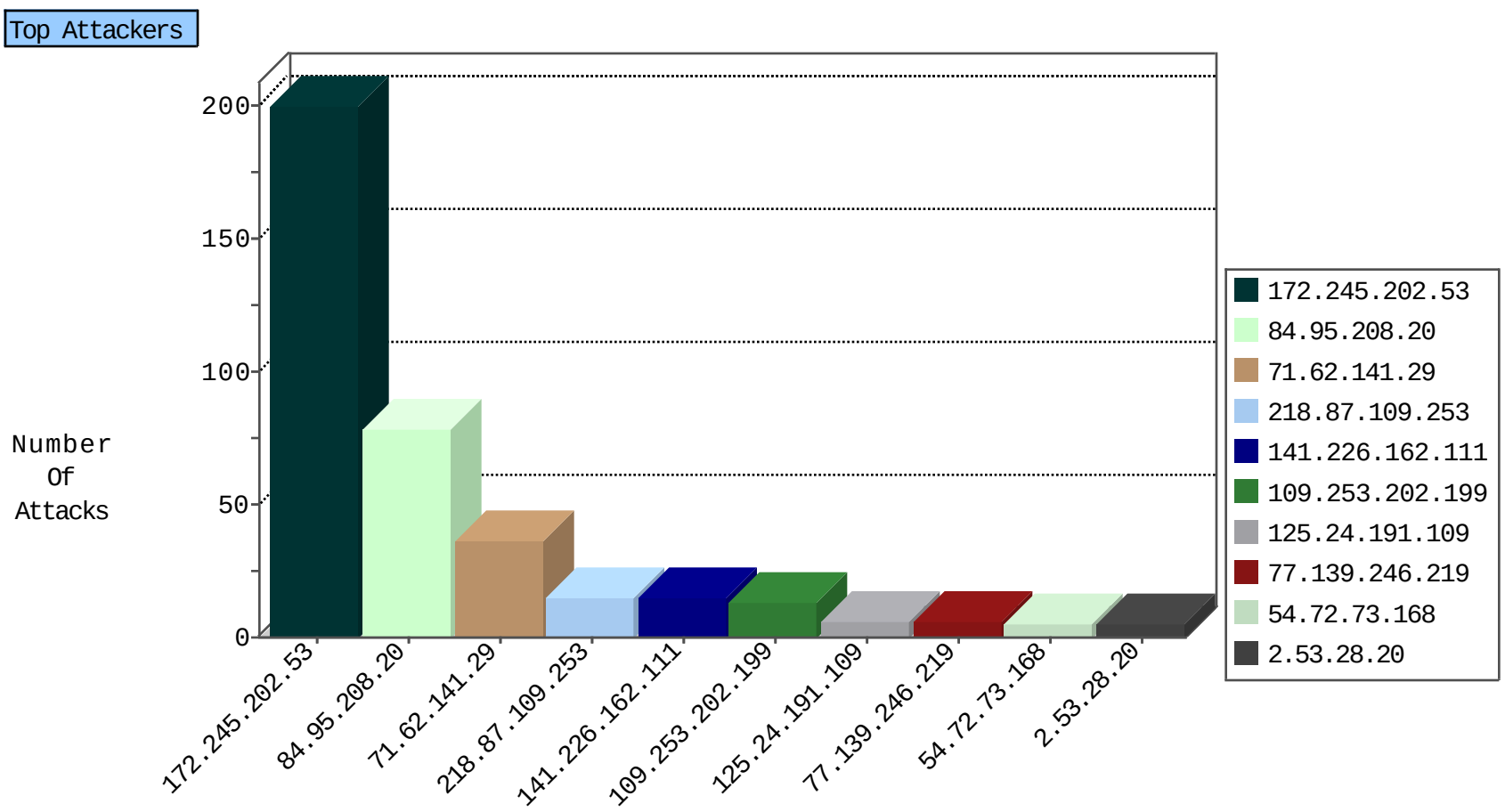
10-02-2016-04:04:07 to 10-02-2016-05:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-02-2016-04:04:07 to 10-02-2016-05:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.177	ncore.idf.il	Black List	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
71.6.146.186	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
188.138.26.214	Germany	147.237.76.86	navy.idf.il	Black List	drop	1
8.37.231.238	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	1
185.94.111.1	Russian Federation	147.237.76.44	e.refuah.idf.il	Black List	drop	1
58.218.200.137	China	147.237.0.17	m.my-kosher-kravi.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
185.94.111.1	Russian Federation	147.237.76.196	e.sviva.idf.il	Black List	drop	1

10-02-2016-04:04:07 to 10-02-2016-05:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.90.210.70	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
69.30.213.202	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

10-02-2016-04:04:07 to 10-02-2016-05:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
14.219.67.91	147.237.72.166	China	aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.87.109.253	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
218.87.109.253	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
66.249.75.48	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
218.87.109.253	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
58.220.2.5	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
46.172.91.20	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.87.109.253	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
24.39.95.126	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
218.87.109.253	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
66.249.65.51	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
218.87.109.253	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
50.116.123.33	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
27.151.137.151	147.237.76.202	China	e.halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.87.109.253	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1

10-02-2016-04:04:07 to 10-02-2016-05:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
172.245.202.53	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	199
141.226.162.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
71.62.141.29	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	8
71.62.141.29	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	7
71.62.141.29	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.253.202.199	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	7
71.62.141.29	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
71.62.141.29	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
125.24.191.109	Thailand	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
141.226.162.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.28.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
84.109.1.247	Israel	147.237.72.166	aka.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
109.253.202.199	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
207.46.13.7	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.76.108	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.202.199	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
77.139.246.219	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.139.246.219	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
77.139.246.219	France	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
47.16.89.15	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.2	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
91.55.182.9	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
70.174.110.37	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
46.19.86.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
156.198.172.68	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
108.30.253.193	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
70.174.110.37	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
176.13.18.183	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.86.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
163.172.220.201	United Kingdom	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.71	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.65.134.84	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
74.82.47.6	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
70.174.110.37	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
163.172.220.201	United Kingdom	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.86.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
79.181.99.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.105.247.224	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
85.65.134.84	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.40	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
70.174.110.37	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1

10-02-2016-04:04:07 to 10-02-2016-05:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	74
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
66.249.65.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9366-he/refuah.aspx	Block	1
207.46.13.98	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/drushim/info.aspx	None	1
67.83.74.126	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
66.249.65.8	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/apple-app-site-association	Block	1
157.55.39.145	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chinuch/contact/	None	1
66.249.65.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
207.46.13.98	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/haredim/gallery.aspx	None	1
68.180.229.184	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
66.249.65.10	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/assetlinks.json	Block	1
157.55.39.196	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/general.aspx	Block	1
66.249.66.101	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
207.46.13.98	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/sachar/faq.aspx	None	1
66.249.65.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
180.76.15.136	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/shared/clientscripts/jquery/' + url + '	Block	1
66.249.76.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim1/main02f1.html	Block	1
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
204.79.180.71	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/showpicture.asp	Block	1
104.237.156.66	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/2113-	Block	1

10-02-2016-04:04:07 to 10-02-2016-05:04:07