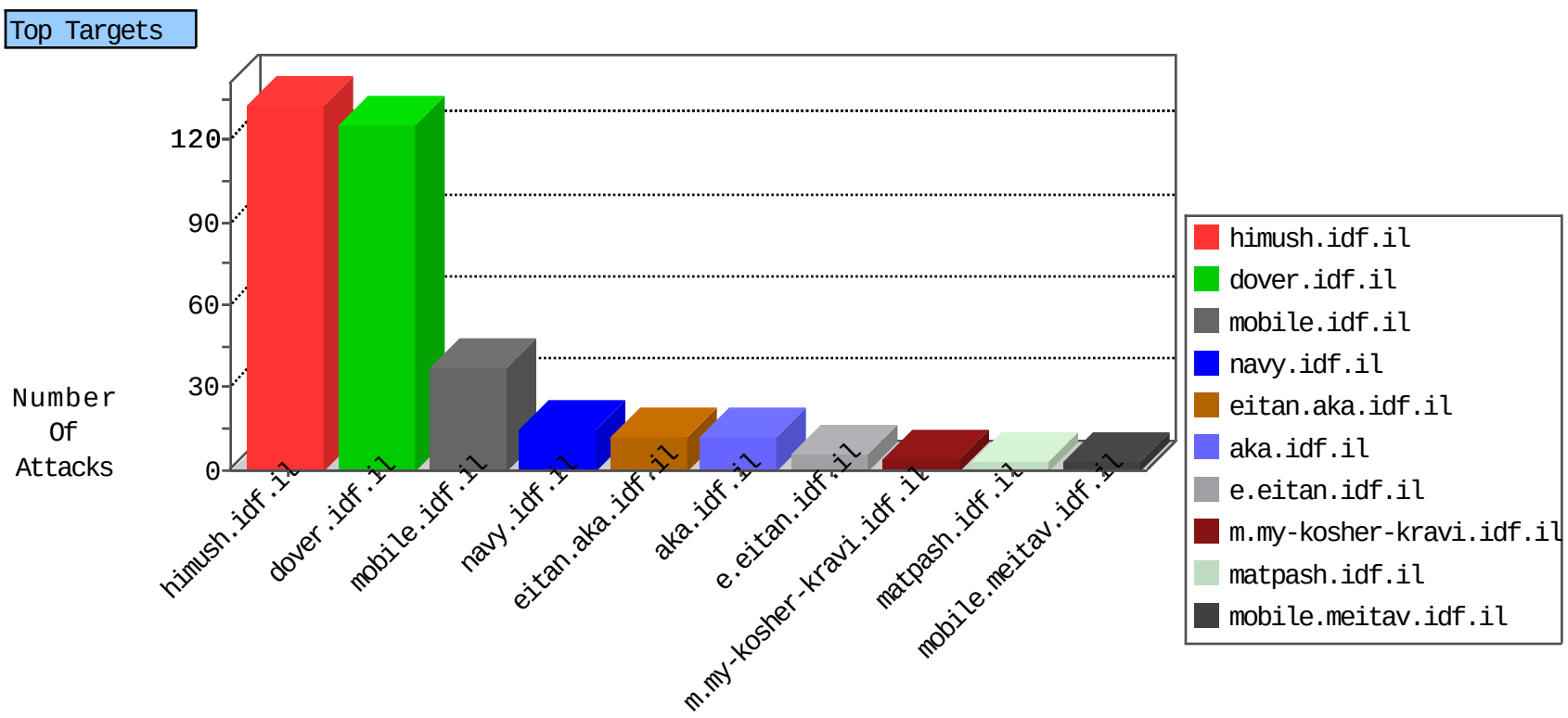
10-03-2016-07:04:06 to 10-03-2016-08:04:06

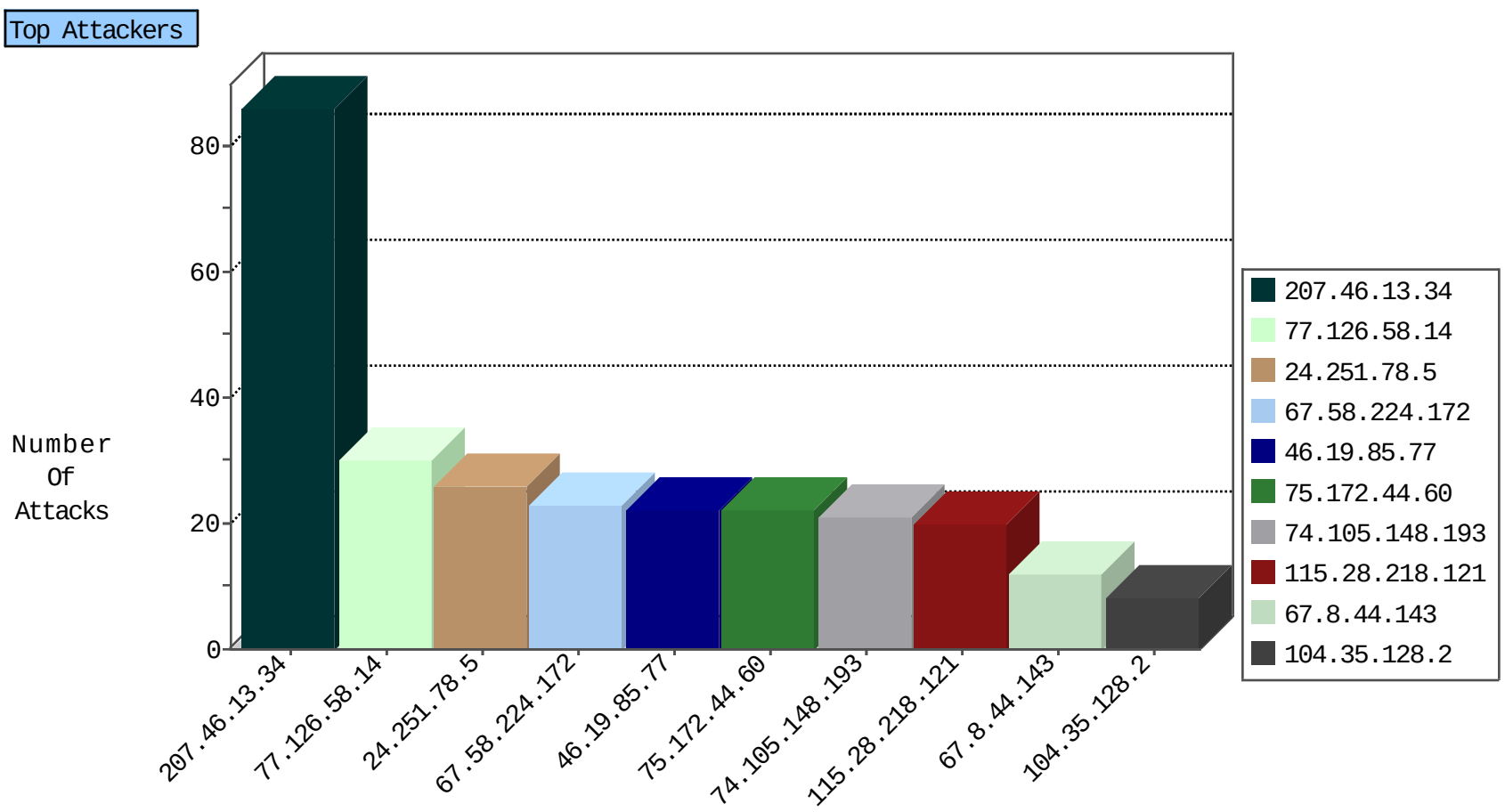
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-03-2016-07:04:06 to 10-03-2016-08:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.177.164.99	Romania	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
209.126.136.2	United States	147.237.76.86	navy.idf.il	Black List	drop	1

10-03-2016-07:04:06 to 10-03-2016-08:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
92.156.117.102	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
69.30.221.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

10-03-2016-07:04:06 to 10-03-2016-08:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
202.170.80.40	147.237.76.177	Mongolia	ncore.idf.il	ET SCAN Potential SSH Scan	1
14.177.180.2	147.237.77.61	Vietnam	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
139.162.246.121	147.237.76.196	United States	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
14.177.180.2	147.237.8.46	Vietnam	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
14.177.180.2	147.237.0.33	Vietnam	idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.59.11	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
85.143.216.168	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
45.33.124.223	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
14.177.180.2	147.237.77.233	Vietnam	atal.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.76.34	United States	yohalan.idf.il	ET DROP Dshield Block Listed Source	1
14.177.180.2	147.237.76.30	Vietnam	himush.idf.il	ET SCAN Potential SSH Scan	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
14.177.180.2	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
14.177.180.2	147.237.0.16	Vietnam	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
5.255.90.133	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
66.249.69.108	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	1
221.235.191.202	147.237.76.196	China	e.sviva.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
45.33.124.223	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential SSH Scan	1

10-03-2016-07:04:06 to 10-03-2016-08:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	86
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
24.251.78.5	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
67.58.224.172	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
75.172.44.60	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
74.105.148.193	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
67.8.44.143	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
104.35.128.2	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
104.50.183.111	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
49.228.227.69	Thailand	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
115.28.218.121	China	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.77	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.77	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.187.72	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
115.28.218.121	China	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
115.28.218.121	China	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
115.28.218.121	China	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
2.53.133.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
115.28.218.121	China	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	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
64.246.178.34	United States	147.237.76.86	navy.idf.il	Header Rejection	header rejection pattern found in request	monitor	2
162.209.232.47	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
109.67.104.115	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
188.247.79.215	Jordan	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
52.198.122.46	Japan	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.13.232.124	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
89.248.174.4	Netherlands	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
200.79.231.62	Mexico	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.16	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.222	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
162.209.233.37	United States	147.237.0.200	m4u.idf.il	drop		drop	1
216.218.206.106	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
192.168.173.102		147.237.77.216	dover.idf.il	drop		drop	1
184.105.139.79	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
138.246.253.19	Germany	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
89.248.174.4	Netherlands	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1
200.79.231.62	Mexico	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
74.82.47.23	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
50.184.58.34	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
172.247.84.215	United States	147.237.0.33	idf.il	drop		drop	1
23.224.172.54	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
216.218.206.106	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.109.88.222	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
192.223.25.79	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.204	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
138.246.253.19	Germany	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.76.54	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding Gb&T907@)DKd&f^z^H!1kR[[#28]]{	None	1
89.248.172.16	Netherlands	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/robots.txt	Block	1
207.46.13.102	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
66.249.79.102	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
128.68.26.56	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
68.180.230.186	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
173.231.185.150	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/admin/i18n/readme.txt	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
79.177.55.176	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
173.231.185.150	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/admin/i18n/readme.txt	Block	1
66.249.76.54	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Parameter Name Gb&T907@)DKd&f^z^H!1kR[[#28]]{	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
180.153.228.91	China	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/	Block	1