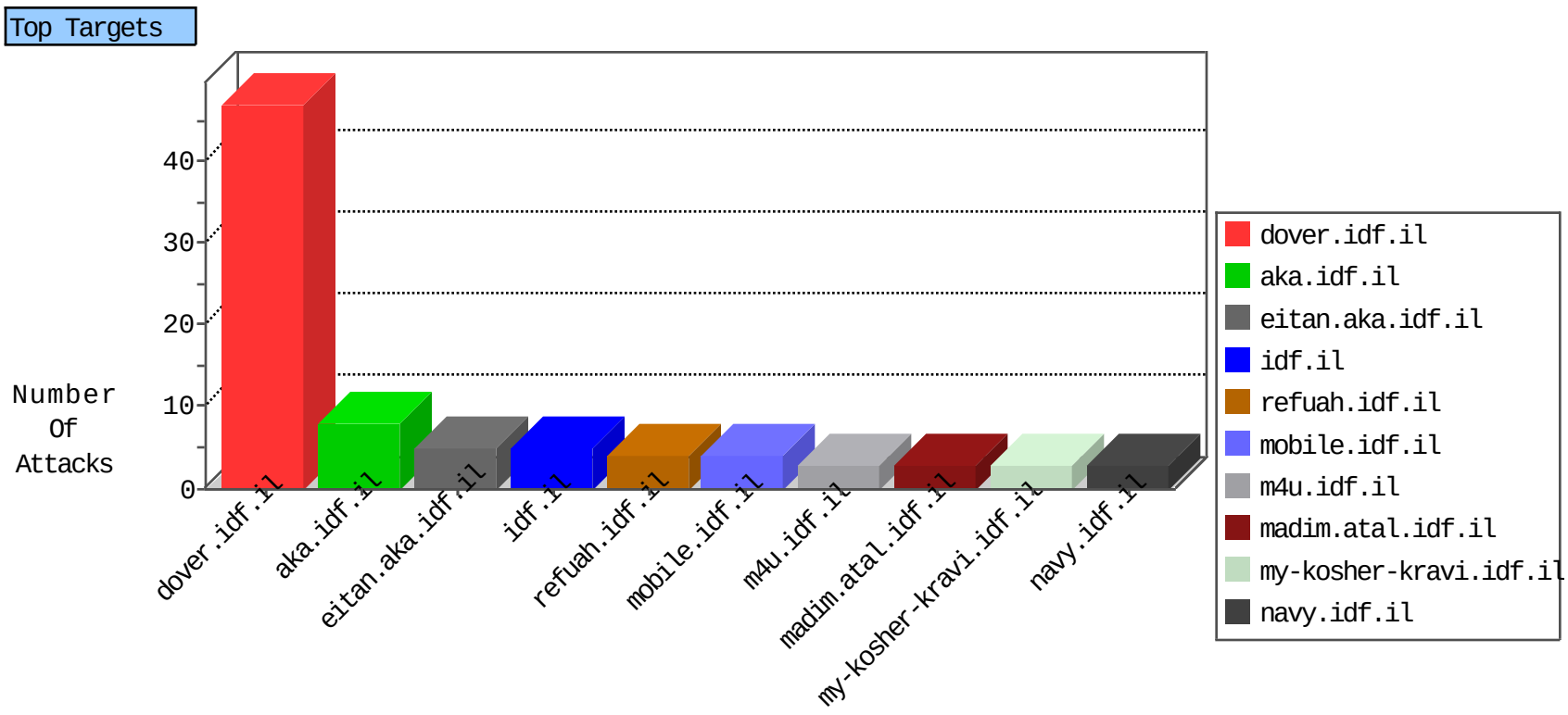
10-04-2016-06:04:03 to 10-04-2016-07:04:03

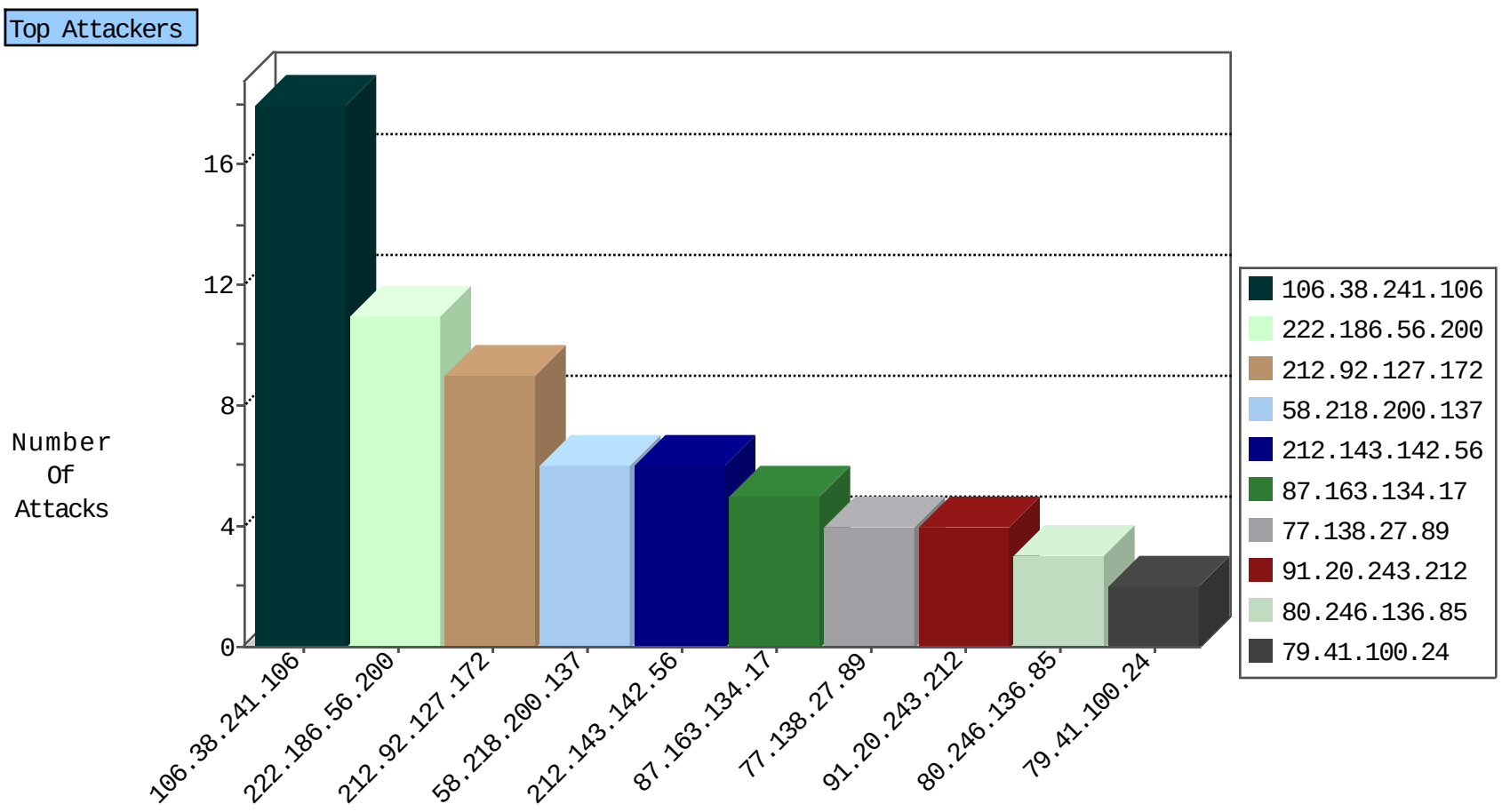
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

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

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
124.129.0.26	China	147.237.8.14	e.orchot.idf.il	Invalid TCP Flags	drop	1
124.129.0.26	China	147.237.8.45	e.eitan.idf.il	Invalid TCP Flags	drop	1
218.84.233.53	China	147.237.76.31	nakchal.idf.il	Black List	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	18

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

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
222.186.56.200	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
146.200.148.0	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
91.121.78.198	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
222.186.56.200	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	2
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
87.163.134.17	147.237.0.33	Germany	idf.il	ET SCAN Potential SSH Scan	2
58.218.200.137	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.200	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.200.137	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.200	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
200.58.214.138	147.237.8.28	Colombia	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
45.32.194.53	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
14.152.59.11	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
87.163.134.17	147.237.0.19	Germany	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.200	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.163.134.17	147.237.0.16	Germany	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.200	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.200.137	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.200	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.200.137	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
219.146.251.139	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
200.58.214.138	147.237.8.28	Colombia	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
45.32.194.53	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.76.86	Canada	navy.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.59.11	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.200	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.163.134.17	147.237.0.17	Germany	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
222.186.56.200	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.79.107	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1

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

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	6
77.138.27.89	France	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.20.243.212	Germany	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
80.246.136.85	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
2.53.25.128	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
79.41.100.24	Italy	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
2.55.154.146	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
8.21.198.25	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.180.229.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
187.61.124.12	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.16.83	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
212.92.127.172	Russian Federation	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
188.120.148.84	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	1
45.56.102.167	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.218.206.104	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
212.92.127.172	Russian Federation	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
183.129.160.229	China	147.237.72.14	dover.idf.il(old	drop	SAM rule	drop	1
212.92.127.172	Russian Federation	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.218.206.120	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
212.92.127.172	Russian Federation	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
183.129.160.229	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
213.149.62.215	Croatia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
212.92.127.172	Russian Federation	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.102	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
212.92.127.172	Russian Federation	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.99.32.146	Lebanon	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
85.250.214.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.70	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
212.92.127.172	Russian Federation	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.103	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
71.6.167.142	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
212.92.127.172	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
87.69.143.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.76	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
212.92.127.172	Russian Federation	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.180	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
66.249.66.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
66.249.69.72	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1284-he/refuah.aspx	Block	1
66.249.75.54	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/801-he/patzar	Block	1
66.249.64.164	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1

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