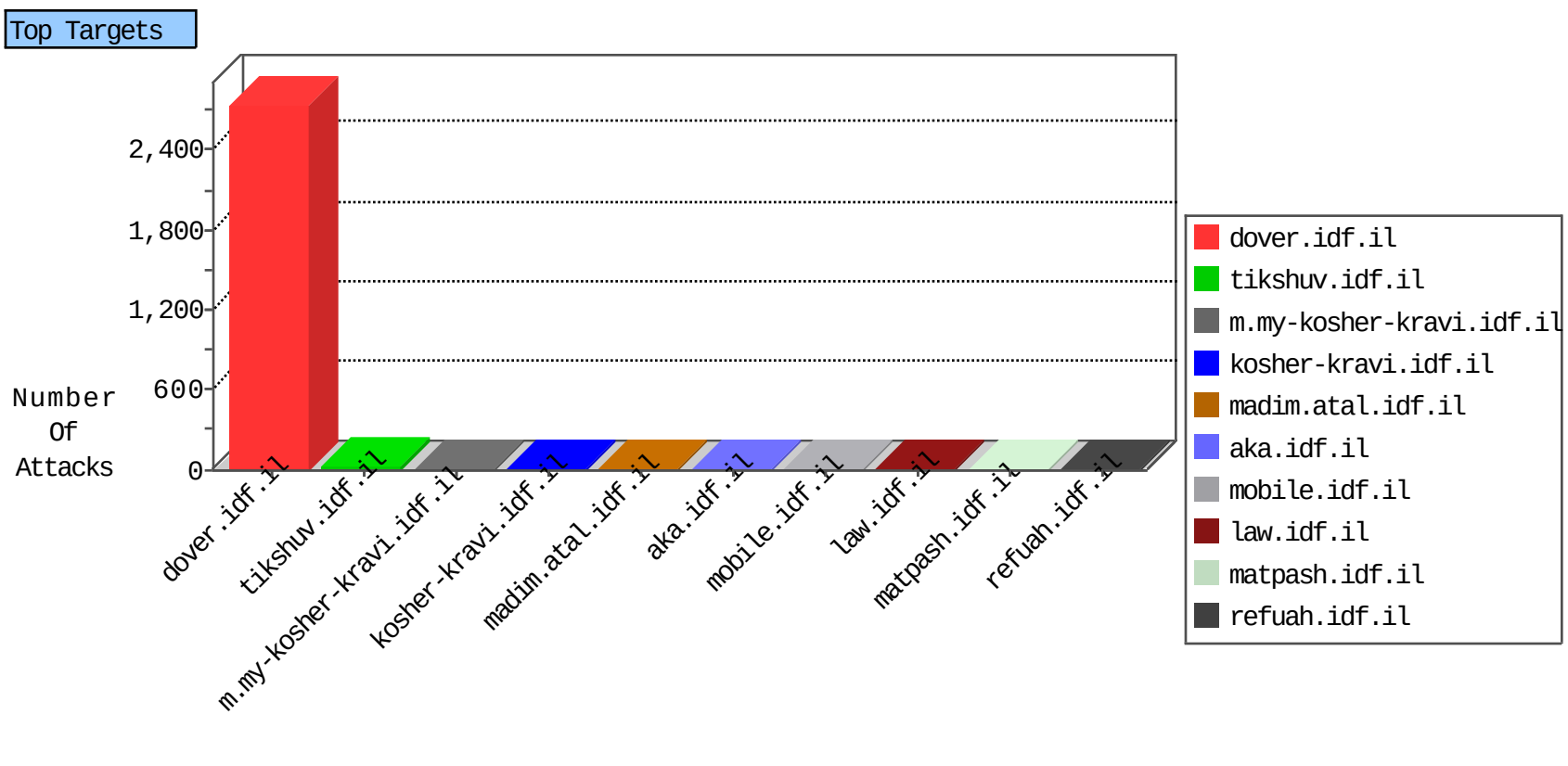
03-14-2016-03:04:06 to 03-14-2016-04:04:06

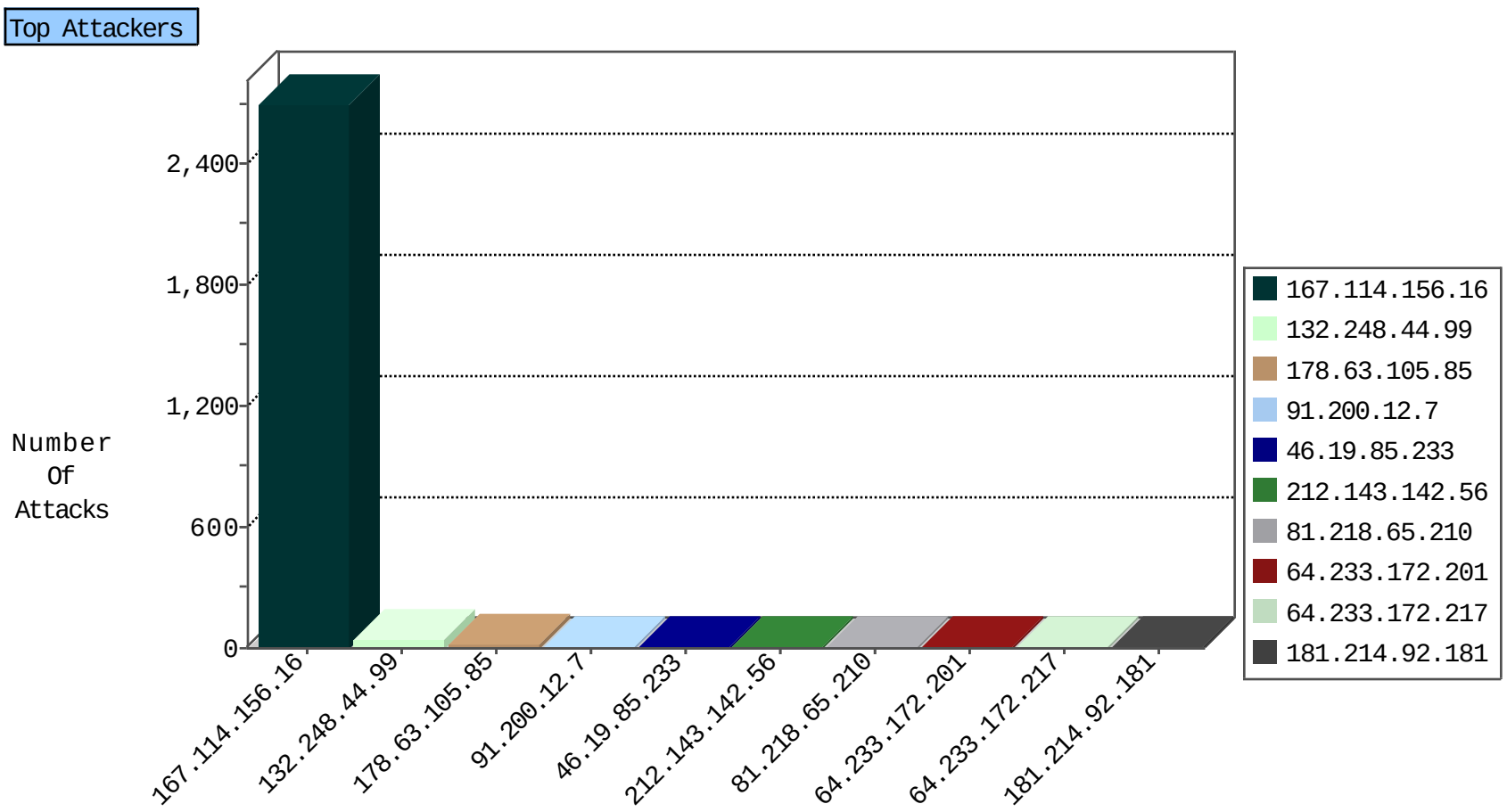
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

03-14-2016-03:04:06 to 03-14-2016-04:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3719
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
172.106.7.194		147.237.76.39	mobile.meitav.idf.il	L4 Source or Dest Port Zero	drop	1

03-14-2016-03:04:06 to 03-14-2016-04:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
132.248.44.99	Mexico	147.237.0.17	m.my-kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	10
132.248.44.99	Mexico	147.237.0.15	kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	10
132.248.44.99	Mexico	147.237.0.19	madim.atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
132.248.44.99	Mexico	147.237.0.15	kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	2
132.248.44.99	Mexico	147.237.0.17	m.my-kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	2
66.249.64.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
132.248.44.99	Mexico	147.237.0.19	madim.atal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

03-14-2016-03:04:06 to 03-14-2016-04:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
132.248.44.99	147.237.0.15	Mexico	kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	2
132.248.44.99	147.237.0.17	Mexico	m.my-kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	2
181.214.92.181	147.237.77.212	Chile	e.dover.idf.il	ET SCAN Potential SSH Scan	1
132.248.44.99	147.237.0.19	Mexico	madim.atal.idf.il	ET WEB_SERVER Muieblackcat scanner	1
82.117.208.243	147.237.72.156		aman.idf.il	ET SCAN NMAP -sS window 1024	1
58.253.96.122	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
47.23.96.141	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 2048	1
211.20.129.79	147.237.76.31	Taiwan	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
193.105.134.220	147.237.77.61	Sweden	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
181.214.92.181	147.237.77.233	Chile	atal.idf.il	ET SCAN Potential SSH Scan	1
181.214.92.181	147.237.77.179	Chile	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
58.253.96.122	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 4096	1
47.23.96.141	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
218.246.0.97	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
47.23.96.141	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -f -sS	1
181.214.92.181	147.237.77.235	Chile	sviva.idf.il	ET SCAN Potential SSH Scan	1

03-14-2016-03:04:06 to 03-14-2016-04:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
64.233.172.201	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
64.233.172.217	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.7	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
2.54.172.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.193	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.66.60.75	Denmark	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.233	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	2
64.46.23.242	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	2
46.19.86.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.85.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	2
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	2
141.212.122.168	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.112	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
204.79.180.151	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.27	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.75	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.92	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
76.23.178.61	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.100	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.240.192.138	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.172	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.116	United States	147.237.0.33	idf.il	drop		drop	1
132.248.44.99	Mexico	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
204.79.180.151	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
74.82.47.32	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
141.212.122.77	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.94	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
76.23.178.61	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.108	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
178.63.105.85	Germany	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	1
46.120.66.169	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.173	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.116	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.68	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.35	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.67	United States	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
173.48.206.163	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.78	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.98	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

03-14-2016-03:04:06 to 03-14-2016-04:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.157.57.9	Sweden	147.237.72.166	aka.idf.il	Unknown Parameter amp;pageNum in www.aka.idf.il/iturim/asp/wars.asp	None	1
141.212.122.64	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /x	Block	1
42.60.44.12	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
216.65.160.141	Canada	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.75.16	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9043-he/refuah.aspx	Block	1
31.210.187.162	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
157.55.39.49	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.249.75.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/scroller/skin.css	Block	1
37.26.149.245	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
157.55.39.155	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.155	Block	1
66.249.65.125	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter tab in www.eitan.aka.idf.il/938-en/eitan.aspx	None	1
71.43.100.242	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/).html(	Block	1
38.111.147.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
157.55.39.155	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/	Block	1
66.249.69.84	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
141.212.122.64	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /x	Block	1
40.77.167.11	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
204.79.180.249	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1

03-14-2016-03:04:06 to 03-14-2016-04:04:06