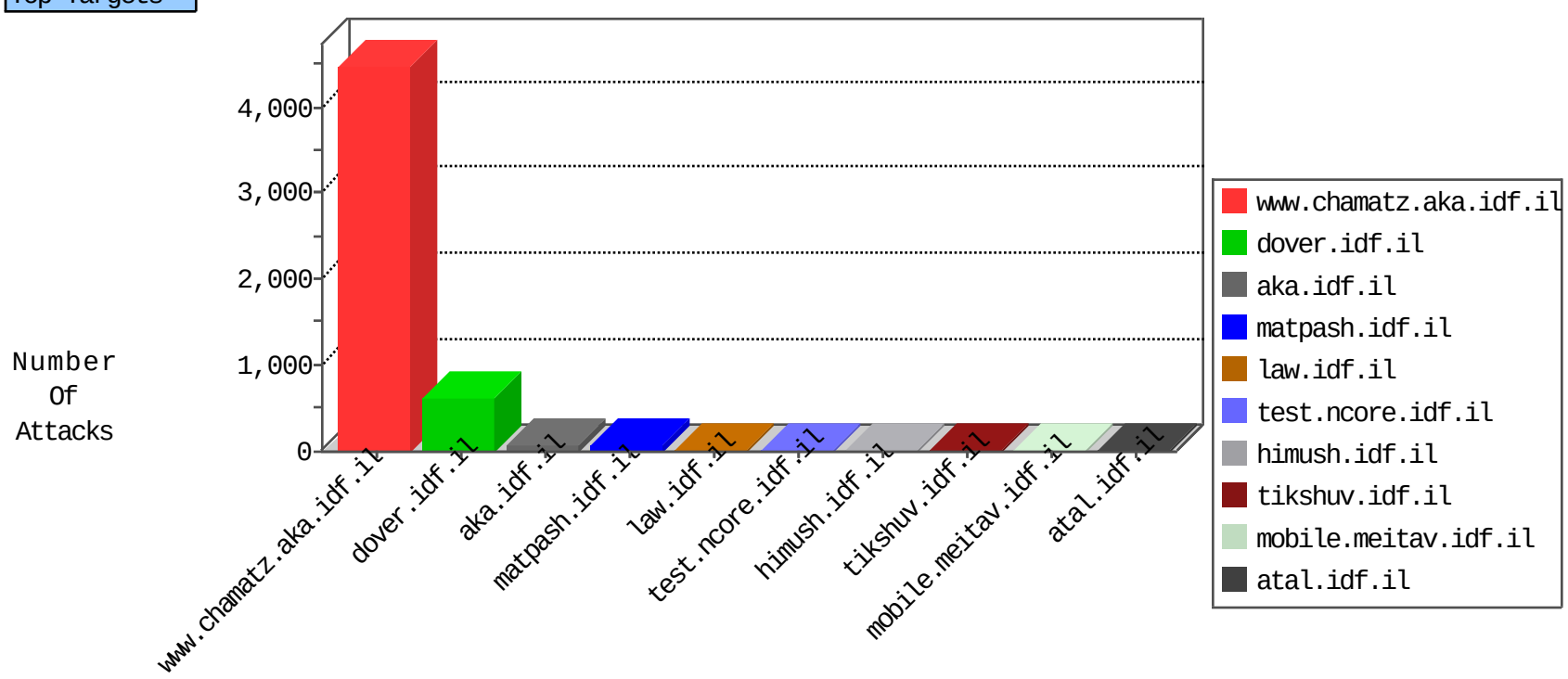
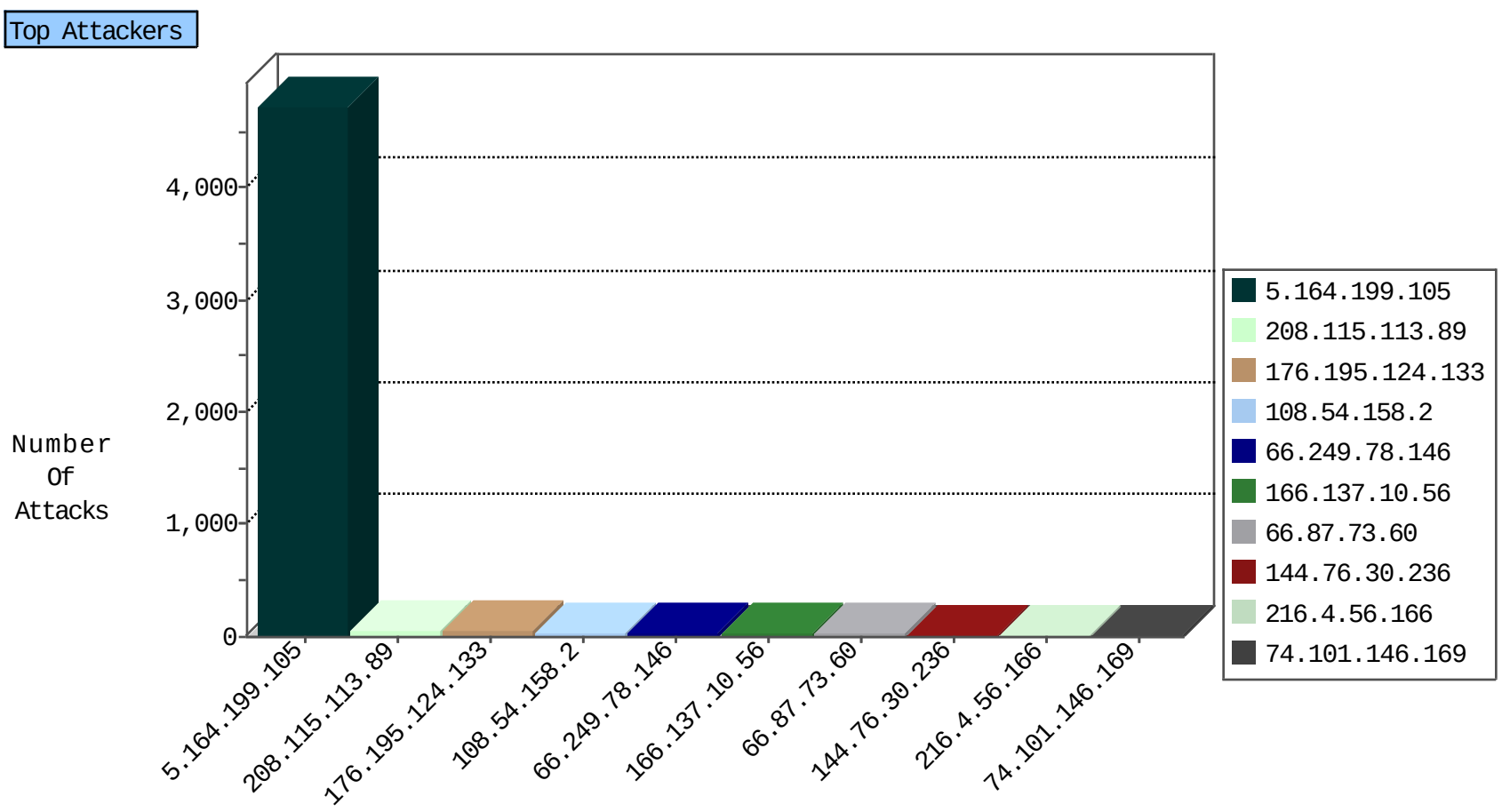
04-26-2016-05:04:09 to 04-26-2016-06:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-26-2016-05:04:09 to 04-26-2016-06:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.164.199.105	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9503
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
72.5.195.35	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
183.60.48.25	China	147.237.76.38	e.e.meitav.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

04-26-2016-05:04:09 to 04-26-2016-06:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-26-2016-05:04:09 to 04-26-2016-06:04:09

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
112.196.49.101	147.237.77.176	India	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
112.196.49.101	147.237.77.176	India	matpash.idf.il	ET SCAN NMAP -f -sS	1
202.29.86.129	147.237.76.44	Thailand	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.76.44		e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.204.211	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.204.211	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
173.65.154.27	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
117.20.41.62	147.237.76.201	Singapore	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.77.176	India	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
202.29.86.129	147.237.77.233	Thailand	atal.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.76.38	Turkey	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.76.38	United States	e.e.meitav.idf.il	ET DROP Dshield Block Listed Source	1
80.82.78.38	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.48	147.237.77.234	Lithuania	halag.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.204.211	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
174.37.194.144	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
163.172.8.19	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1

04-26-2016-05:04:09 to 04-26-2016-06:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.164.199.105	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4467
5.164.199.105	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	242
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
176.195.124.133	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	50
108.54.158.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
166.137.10.56	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.87.73.60	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
144.76.30.236	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
216.4.56.166	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	19
74.101.146.169	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
157.55.39.74	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
38.111.147.84	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.21.178.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.164.199.105	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.75.79.141	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.21.15.183	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
50.18.94.121	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.173.94.51	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.22.4.232	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
24.120.55.18	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.246	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
17.142.156.109	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
174.37.194.144	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
82.80.27.79	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.81.228	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
119.92.61.47	Philippines	147.237.76.39	mobile.meitav.idf.il	drop	First packet isn't SYN	drop	3
84.228.223.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.49.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.184	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.183.191.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.55.7.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.247	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.92.72.16	Netherlands	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
8.37.228.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.78.206	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
119.92.61.47	Philippines	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	3
68.114.120.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
157.55.39.48	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/undefined	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
185.92.72.16	Netherlands	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/clientscripts.js	Block	1
71.232.32.171	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
5.153.234.154	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
185.92.72.16	Netherlands	147.237.77.235	sviva.idf.il	Unauthorized URL Access to www.hagnas.atal.idf.il/hnap1/	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.scrollfollow.js	Block	1
79.178.233.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
5.153.234.154	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
207.46.13.32	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9064-he/refuah.aspx	Block	1
81.223.254.34	Austria	147.237.0.34	tikshuv.idf.i	Unauthorized URL Access to /robots.txt	Block	1
38.111.147.84	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
216.218.206.66	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
68.180.230.108	United States	147.237.76.31	nakchal.idf.i	Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1