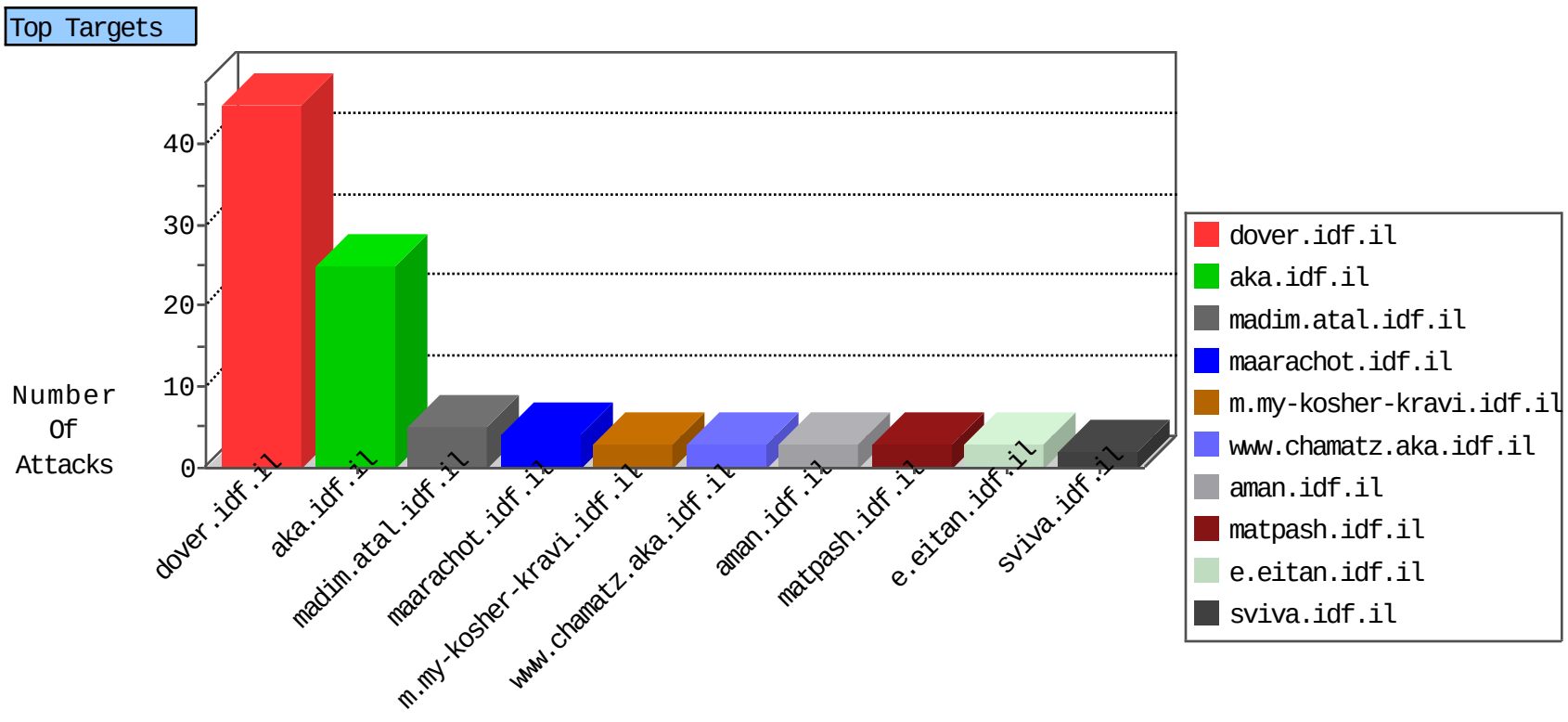
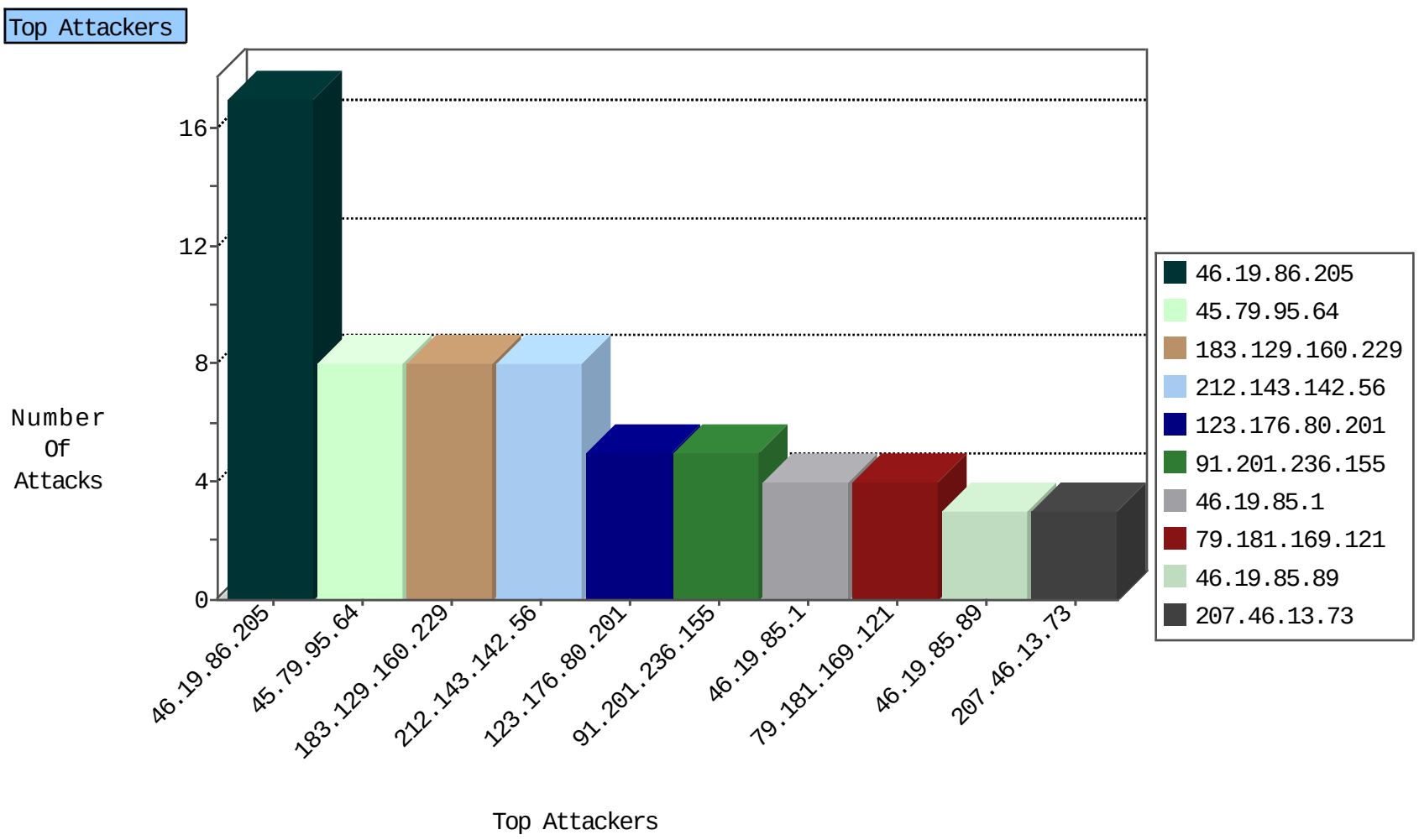
09-04-2016-02:04:05 to 09-04-2016-03:04:05

IDF Under Attack
Daily Report





09-04-2016-02:04:05 to 09-04-2016-03:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-04-2016-02:04:05 to 09-04-2016-03:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-04-2016-02:04:05 to 09-04-2016-03:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
45.79.95.64	147.237.77.216	United States	dover.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
37.8.118.98	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	1
123.176.80.201	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.155	147.237.77.226	Ukraine	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.155	147.237.76.197	Ukraine	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
193.201.225.73	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
87.236.194.161	147.237.0.19	Czech Republic	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
183.129.160.229	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
50.116.123.135	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.238.44	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.172	147.237.0.17	Sweden	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
123.176.80.201	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 1024	1
45.79.71.122	147.237.77.170	United States	maarachot.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
123.176.80.201	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
123.176.80.201	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.77.226	Ukraine	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
87.236.194.161	147.237.77.205	Czech Republic	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.73	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
72.252.24.133	147.237.72.156	Jamaica	aman.idf.il	ET SCAN NMAP -sS window 4096	1
177.200.192.50	147.237.77.235	Brazil	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
50.116.123.135	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.238.43	147.237.0.33	United Kingdom	idf.il	ET SCAN NMAP -sS window 1024	1
123.176.80.201	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

09-04-2016-02:04:05 to 09-04-2016-03:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.205	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	17
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.89	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
46.19.86.3	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
46.19.85.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
183.129.160.229	China	147.237.77.121	e.navy.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
201.179.210.195	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.133.98	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.77.212	e.dover.idf.il	drop	SAM rule	drop	1
109.253.135.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
46.19.85.105	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
212.179.219.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.77.227	e.hamaz.idf.il	drop	SAM rule	drop	1

09-04-2016-02:04:05 to 09-04-2016-03:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.169.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
45.79.95.64	United States	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	2
45.79.95.64	United States	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	2
207.46.13.73	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.221	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
207.46.13.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.85.1	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
144.76.236.183	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
192.222.174.5	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
68.99.6.55	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/iturim/asp/default.asp	Block	1
46.19.85.1	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/general/	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
46.19.85.1	Israel	147.237.77.216	dover.idf.il	Malformed URL __atssc=facebook;1	Block	1
157.55.39.71	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
66.249.79.116	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/faq/faq.aspx	Block	1
45.79.95.64	United States	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 4	Block	1
207.46.13.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_moreinfo.asp	Block	1
77.138.198.203	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
46.19.85.1	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 7cb5a620650a321000; in URL __atssc=facebook	Block	1
66.249.85.179	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
45.79.95.64	United States	147.237.77.216	dover.idf.il	Multiple Malformed HTTP Header Line from 45.79.95.64	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
157.55.39.244	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/home/default.aspx	Block	1
68.99.6.55	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 68.99.6.55	Block	1

09-04-2016-02:04:05 to 09-04-2016-03:04:05