Spybot Anti-Beacon

Spybot Anti-Beacon is an application that scans for telemetry services in your Windows desktop clients. Telemetry services log system and usage data and upload the data to remote servers for monitoring. Microsoft and other software companies are in this vein "calling back home". Since the Windows XP age this was always considered to be a problem by privacy conscious users. Anti-Beacon checks for numerous data collecting services and blocks them through an easy to use Immunization process.

We launched Anti-Beacon back in 2015 (28-08-2015) as part of the Spybot application family to make your privacy more secure. Our most recent version is Spybot Anti-Beacon 3.5 and was released on 05-02-2020. Anti-Beacon Free offers up to 206 immunizing objects checks, the Plus edition adds more than 83 extra telemetry checks (depending on your system configuration).

How to use Anti-Beacon?

This is easy, simply install and leave the option "Refresh immunization after each system restart" checked. The main application page of Anti-Beacon shows a big progress circle with the current immunization information. By clicking on the circle you will enter the telemetry options page with all listed immunizers. Here you can either block individual telemetry objects or choose a predefined blacklist via the "Protection Preset" button. By selecting "Apply" you can activate your telemetry blocking set. This immunization set will be enforced on every reboot.

What is Telemetry?

Telemetry is the automatic process of usage data acquisition and the broadcast of the data to a dedicated application or a remote server. Collected telemetry data is used among other things for debugging, performance and usage monitoring, even security analysis.

Microsoft describes telemetry gathering as a diagnostic data collection to enhance Microsoft products and services:

> *Windows 10 collects Windows diagnostic data—such as usage data, performance data, inking, typing, and utterance data—and sends it back to Microsoft. That data is used for keeping the operating system secure and up-to-date, to troubleshoot problems, and to make product improvements.*
>
> *Source: https://docs.microsoft.com/en-us/windows/privacy/windows-personal-data-services-configuration*

What is Immunization?

Immunization disables active telemetry objects for Windows and selected applications. This Immunization process is started on every system start and automatically re-blocks (refreshes) each unwanted telemetry item or group, if necessary. Telemetry functions are disabled through Anti-Beacon by configuration and the editing of Windows Configuration Options, Firewall Settings, Group Policies, HOSTS Files, System Services and/or Scheduled Task. Anti-Beacon deactivates all known telemetry objects but does not delete anything to allow a fallback to original Windows settings.

What kind of immunizing categories are supported in Anti-Beacon Free?

Anti-Beacon Free offers basic immunizing objects in the following categories: Operating System, Third Party Analytics, and Antivirus.

What kind of immunizing categories are supported in Anti-Beacon Plus?

The Plus version offers further immunizing objects in the following categories: Preinstalled Manufacturer Software, Browser, Office, and Development.

Versions and Pricing

Anti-Beacon 3.5 is available in 2 editions: Free and Plus.

The Free version offers all basic immunizers and is free for private Users. A Plus license adds 80+ telemetry objects to your immunization. Anti-Beacon Plus 3.5 can be purchased individually for €7.99 / $9.99.

The Anti-Beacon Plus license is included in Spybot Professional, Corporate and Technician's Editions. Standard and portable installers are available for your convenience.

Links:

https://www.safer-networking.org/products/spybot-anti-beacon/
https://www.safer-networking.org/support/spybot-anti-beacon-faq/