BUY

24 Aug 2020

Conduct Investigations Securely and Privately Using Maltego's Stealth Mode

Maltego Team

When running Transforms to return pivots and information in an investigation it is often important that investigators avoid direct contact with the target's servers or networks for a number of reasons. For example, leaving footprints in the target network's traffic logs could alert the suspects and, as a result, an investigator may lose important leads. In another scenario, a target's malware may have a built-in "kill switch" or anti-analysis defense mechanism that shuts it down once it detects an otherwise unresponsive query likely triggered by investigators.

How Maltego Keeps Investigators Anonymous

Used by experts in various industries such as cybersecurity, trust and safety, and law enforcement, Maltego operates with a number of privacy measures to ensure the anonymity of our users. Maltego does not store users' Transform query details, nor do we reveal users' identifiable information while they are running Transforms or mining data from public OSINT sources or from online intelligence sources.

The Maltego Desktop Client uses our public Commercial Transform Application Server (CTAS) to run Maltego Standard Transforms for gathering OSINT from common sources on the Internet, querying DNS servers, search engines, social networks, various APIs and other

(namely the Maltego Desktop application) remains hidden.

The CTAS can be deployed on premise to avoid the sending of data through Maltego's servers, alternatively users can run Transforms on their own data independent of the internet.

Toggling Privacy Modes on the Maltego Desktop Client

The Maltego Desktop Client provides two privacy modes: Normal and Stealth mode.

During the initial configuration of a new installation, users will be prompted to choose their preferred privacy mode.
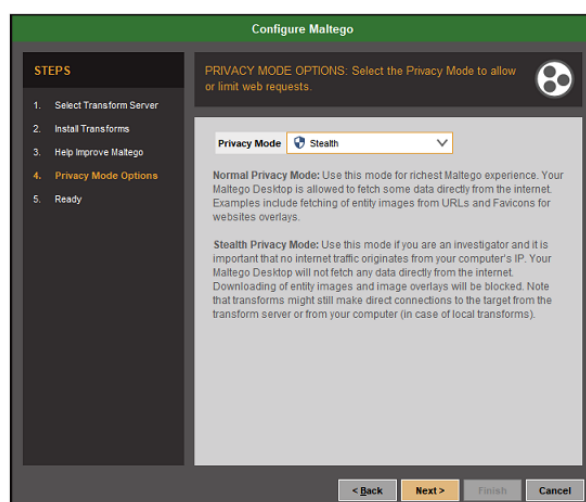
Following the initial set-up, users are able to toggle between the two privacy modes during their investigations using the Privacy Mode dropdown options in the primary tool bar's Investigate tab.

BUY

Maltego public Transforms run through the CTAS server, and while both privacy modes maintain users' anonymity, there is one slight difference.

Normal Privacy Mode

Normal Privacy Mode is designed to provide users with the richest Maltego experience. During an investigation, this mode allows the Maltego Desktop Client to fetch certain data types directly from the internet.

For example, when a URL Entity is returned as an Image Entity, the Maltego Desktop Client fetches the images directly. When a Website Entity is returned, the Client fetches the website favicon from the website and displays it as an Entity overlay.

The graph below shows an example of website favicon overlays and images fetched from URLs.

These fetches are made directly by the Maltego Desktop Client and they bypass our servers. In general, it is safe to keep Maltego activities under Normal Privacy Mode. However, when these fetches happen, a computer's IP might be exposed in the target's traffic log. Therefore, care should be taken when investigating URLs for targets who should not be alerted.

Stealth Mode

BUY

Entity image or website overlay will be blocked.

If sensitive investigations are being conducted, under strict confidentiality practices, or users are simply concerned about exposing their IP, it is recommended that users operate Maltego using Stealth Mode.

BUY

computer during data queries.

Be Aware of Your Privacy Settings

While Maltego continuously works to ensure the security of our users' investigative environments, we do recommend that all our users be aware of their personal privacy needs and ensure that they take the appropriate measures to protect their anonymity.

For more information about Maltego's Normal and Stealth Modes, please refer to our documentation. If you have any questions regarding our privacy practices, feel free to reach out to us at support@maltego.com anytime.

For the latest use cases, product updates and news, follow Maltego on Twitter and LinkedIn or subscribe to our RSS feed!

Previous   Next

Related Articles

PRODUCT | **TUTORIAL** | **PERSON OF INTEREST INVESTIGATION**

Introducing the New Pipl Transforms for Person of Interest Investigations

BUY

Pick the right product and **get started**.

CHOOSE YOUR SOLUTION

Products & Pricing

Maltego for Professionals

Maltego for Enterprises

Pricing

Get Maltego

Download Maltego

Register for Community Edition

Reset Password for Community Edition

Change Log

Buy Maltego

Buy Online

Get Quote

Data Sources

Transform Hub

BUY

Resources

Support

Careers

Blog

Academic and Non-Profit Program

FAQ

Download Logo

© 2020 by Maltego Technologies.

Legal Notice   Data Privacy   Website Privacy   License Agreement