Untitled Goose Tool

A Hunt and Incident Response Tool for Use in Azure, Azure Active Directory, and Microsoft 365 Environments

March 2023

Overview

The Untitled Goose Tool is a robust and flexible hunt and incident response tool. The tool provides network defenders novel authentication and data gathering methods to use as they interrogate and analyze their Microsoft Azure, Azure Active Directory (AAD), and Microsoft 365 (M365) environments to detect potentially malicious activity. Goose, developed by CISA with Sandia National Laboratories, is freely available on the CISA GitHub Repository.

Why Untitled Goose Tool?

CISA advises network defenders to use Untitled Goose Tool to:

- Export and review AAD sign-in and audit logs, M365 unified audit log (UAL), Azure activity logs, Microsoft Defender for IoT (internet of things) alerts, and Microsoft Defender for Endpoint (MDE) data for suspicious activity.
- Query, export, and investigate AAD, M365, and Azure configurations.

Network defenders attempting to interrogate a large M365 tenant via the UAL may find that manually gathering all events at once is not feasible. Untitled Goose Tool uses novel data gathering methods via bespoke mechanisms. With this tool, network defenders can:

- Extract cloud artifacts from Microsoft's AAD, Azure, and M365 environments without performing additional analytics.
- Perform time bounding of the UAL via `goosey graze`.
- Extract data within those time bounds with `goosey honk`.
- Interrogate and collect data using similar time bounding capabilities for MDE data.

Compatibility

Untitled Goose Tool works with a user's Azure, Azure AD, and M365 environments.

Prerequisites

Untitled Goose Tool requires Python 3.7, 3.8, or 3.9. CISA recommends using this tool within a virtual environment.

Instructions

Untitled Goose Tool is available on CISA's GitHub repository as a Python program with an accompanying PowerShell script. See the README.md file in the Untitled Goose Tool GitHub repository for instructions.

Frequently Asked Questions

1. **What operating systems does Untitled Goose Tool support?**

   Untitled Goose Tool can operate on both Windows and MacOS, but the PowerShell script is recommended for Windows use only.

2. **What should I do with the results?**

   Ingest the JSON results into a Security Information and Event Management (SIEM) tool, web browser, text editor, or a database.

3. **How often should I run the tool?**

   Users can run Untitled Goose Tool once, as a snapshot in time, or routinely. For certain log types, the tool will pick up from the last time the tool was executed.

4. **Do I need to configure the tool before I run it?**

   Yes, you will need to edit the `.conf` file. Please see the README.md file in the Untitled Goose Tool GitHub repository for further instructions.

5. **Will Untitled Goose Tool make changes to the cloud environment?**

   No, the tool is unable to make changes to the cloud environment. It only queries for information.

6. **How long does it take to run the tool?**

   Performance time depends on the size of the cloud environment, the amount of activity, and the specific call set in the configuration file.

7. **I noticed a feature that would be great to add to Untitled Goose Tool. Can I contribute?**

   Yes. CISA welcomes contributions via the Untitled Goose Tool GitHub repository.