GitHub - Script-Nomad/raindance: Reconnaissance tool for Microsoft Office 365

By Script-Nomad

Archived: 2026-04-05 21:24:17 UTC

> A toolkit for enumerating and collecting information from Office 365

```
    \ _( )_ \   \           _( )_  \       \
   _(     )_      _( )_   (     )     \  \
  (_________) \ _(     )_(_     _)
    \  \  \    (_________)________)    \ \   \
\     \  \       \  \  \(__________) \
\            \    \  \  \    \  \ \      \
     \   .  \      \    \   \    \  \     \
\ \_O/     \           \ ,      \      \ \  \
     \  \     \    \    /     \     \O_
     /\_  \           \_\        ,/\/       \
     \          ,    \   \    \    /  \  \
  ___     \           __ /O\      \ \         \
 |  _ \ __ _(_)_ __ |  _ \  __ _ _ __   ___ ___
 | |_) / _  | | '_ \| | | |/ _  | '_ \ / __/ _ \
 |  _ < (_| | | | | | |_| | (_| | | | | (_|  __/
 |_| \_\__,_|_|_|_| |_|____/ \__,_|_| |_|\___\___|
            - Office 365 Info-Gathering Toolkit
```

Latest Updates

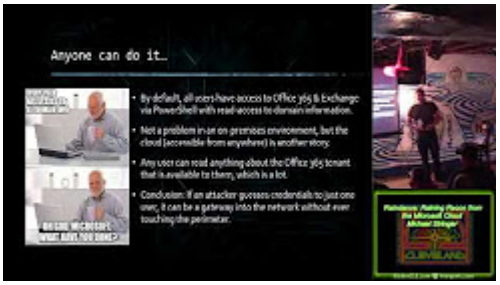
Sorry for the delay in updates. I've been working on a cross-platform/python implementation to replace this, but it's slow going as I am doing some cert-chasing and swamped with other projects. There are some tentatively tested changes in dev, but they haven't been thoroughly put through the wringer yet. Mileage may vary. Thanks for the support 👍

Description

Raindance uses built-in powershell modules, namely from the MSOnline & AzureAD powershell modules to log into Office 365 tenants with legitimate credentials and pulls out the list of users, their mailing groups and distros, roles/permissions, and identify administrators in the tenant. This tool is intended to be used as an attack tool to assist penetration testers in enumerating users and select targets for offensive engagements.

BSides Talk

I was given the opportunity to speak at BSides about my findings associated with my research into Office 365 that led to the development of Raindance. This video goes into some additional detail of how to use the tool effectively, along with plausible scenarios in which it can be useful. If you are interested in that talk, you can find it here.



Features

- Enumerates domain information within O365
- Get the full list of users, including disabled accounts
- Get a list of the mailing/distribution groups in the tenant
- Identify administrative users and highlight Global Administrators (Company Admins)

In the works

- Support for Exchange Server & Office API login
- Search and download emails (with administrator impersonation)
- Automated password searcher (dig through mail & sharepoint for indicators of plaintext passwords)
- Upload/Download files to/from Sharepoint
- Malicious modification of Sharepoint/OneDrive files
- Remote deployment over psexec

Installation & Running

Raindance runs like a powershell module, and does not require any installation. Simply clone it to a directory, and import as a powershell module to gain access to its functions. It is recommended to run as administrator the first time in order to enable it to install the necessary dependencies, or you may do so manually.

```
 # Open a Powershell Command Window as administrator
# Ensure you have all the necessary dependencies for PowerShell
Set-ExecutionPolicy RemoteSigned

# Install Microsoft Online Services (office 365)
Install-Module MSOnline

# Install AzureAD
Install-Module AzureAD
```

```
# Download & Run raindance
git clone https://github.com/true-demon/raindance.git C:\Path\to\Raindance
cd C:\Path\to\Raindance
Import-Module .\raindance.ps1
```

Dependencies

- Windows Only (for now): Microsoft has promised to (eventually) add Linux support for the library dependencies.
- Powershell v5.0+: This is due to .NET dependencies
- Library - MSOnline: Download using powershell `Install-Module msonline`
- Library - AzureAD: Download using powershell `Install-Module AzureAD`

Optional

It is recommended to install chocolatey for windows to assist with installing Powershell packages

---