Sandbox Report

File: psqlodbc_x64.msi

Resubmit | Print | Download options

SHA-256
a56b6a093fe39ca ... 11e8c96380c77

Submitted by
prashant.deshmukh@fisglobal.com

Discovered

Detonation environment
Windows 10 64, Professional, 10.0 (build 16299)

Network settings
Default network connectivity

Timestamp
Feb. 26, 2024 21:01:10

Threat level
Suspicious

Threat score
75/100

Static analysis | Dynamic analysis | Intelligence | MITRE ATT&CK

File information

Classifications

psqlodbc_x64.msi

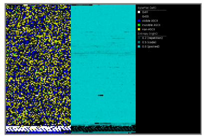
Size	Type	Description	Architecture
5.83MB	msi, data		Unknown

SHA256
a56b6a093fe39ca024e5c819535f608823c568537e24...

Resources

Icon 

Visualization

Input file (PortEx) 

Classification (TrID) 4

80.0% (.MSI) Microsoft Windows Installer

10.7% (.MST) Windows SDK Setup Transform script

7.8% (.MSP) Windows Installer Patch

1.4% (.) Generic OLE2 / Multistream Compound

Risk assessment

Fingerprint 1

Contains ability to retrieve information about the current system

Evasive 1

Marks file for deletion

JSON report

Raw JSON output from the Sandbox detonation


```
{
  "sha256": "a56b6a093fe39ca024e5c819535f608823c568537e24e945711e8c96380cf177",
```

```
  "environment_id": 160,
  "environment_description": "Windows 10 64 bit",
  "file_size": 5967872,
  "file_type": "Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, MSI Installer, Code page: 1252, Title: Installation Database, Subject: psqlODBC_x64, Author: PostgreSQL Global Development Group, Keywords: PostgreSQL, ODBC, Comments: PostgreSQL ODBC Driver, Template: x64;1033, Revision Number: {78AE5022-A9EB-48D5-B652-DDFC32960BCA}, Create Time/Date: Sat Sep 16 08:16:58 2023, Last Saved Time/Date: Sat Sep 16 08:16:58 2023, Number of Pages: 300, Number of Words: 2, Name of Creating Application: W",
  "file_type_short": [
    "msi",
    "data"
  ],
  "submit_name": "psqlodbc_x64.msi",
  "submission_type": "file",
  "verdict": "suspicious",
  "threat_score": 75,
  "windows_version_name": "Windows 10",
  "windows_version_edition": "Professional",
  "windows_version_version": "10.0 (build 16299)",
  "windows_version_bitness": 64,
  "incidents": [
    {
```