Interactivity is now available in beta. Submit or resubmit a file or URL and select 'Live interaction' to explore feature.

Sandbox Report

File: psqlodbc_x64.msi

Resubmit | Print | Download options

SHA-256
a56b6a093fe39ca ... 11e8c96380d177

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

Tactics and Techniques observed

Click on a technique to see additional details.

Execution 1	Persistence 2	Privilege Escalation 3	Defense Evasion 5	Discovery 1	Collection
Native API	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Hijack Execution Flow 1	System Information Discovery	Data Staged 1
	Hijack Execution Flow 1	Hijack Execution Flow 1	DLL Search Order Hijacking		Local Data Staging
	DLL Search Order Hijacking	DLL Search Order Hijacking	Indicator Removal on Host 2		