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 ... 11e8c96380cf177

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

Behavioral threat indicators

Suspicious 21

Contains ability to create directories

Source Hybrid Analysis Technology

Relevance 3/10

MITRE ATT&CK Local Data Staging T1074.001

Details CreateDirectoryW@KERNEL32.dll at 22779-1321-0000000180010E40

Drops DLL executable files (possible DLL search order hijacking)

Source Binary File

Relevance 5/10

MITRE ATT&CK DLL Search Order Hijacking T1574.001

Details [%PROGRAMFILES%\psqlODBC\1600\bin\msvcp140.dll]- [targetUID: 00000000-00007100] "psqlodbc35w.dll" has type "PE32+ executable (DLL) (GUI) x86-64 for MS Windows"- Location: [%PROGRAMFILES%\psqlODBC\1600\bin\psqlodbc35w.dll]- [targetUID: 00000000-00007100] "psqlodbc30a.dll" has type "PE32+ executable (DLL) (GUI) x86-64 for MS Windows"- Location: [%PROGRAMFILES%\psqlODBC\1600\bin\psqlodbc30a.dll]- [targetUID: 00000000-00007100] "libintl-9.dll" has type "PE32+ executable (DLL) (console) x86-64 for MS Windows"- Location: [%PROGRAMFILES%\psqlODBC\1600\bin\libintl-9.dll]- [targetUID: 00000000-00007100] "libpq.dll" has type "PE32+ executable (DLL) (console) x86-64 for MS Windows"- Location: [%PROGRAMFILES%\psqlODBC\1600\bin\libpq.dll]- [targetUID: 00000000-00007100] "vcruntime140.dll" has type "PE32+ executable (DLL) (console) x86-64 for MS Windows"- Location: [%PROGRAMFILES%\psqlODBC\1600\bin\vcruntime140.dll]- [targetUID: 00000000-00007100] "libwinpthread-1.dll" has type "PE32+ executable (DLL) (console) x86-64 (stripped to external PDB) for MS Windows"- Location: [%PROGRAMFILES%\psqlODBC\1600\bin\libwinpthread-1.dll]- [targetUID: 00000000-00007100] "pgxalib.dll" has type "PE32+ executable (DLL) (GUI) x86-64 for MS Windows"- Location: [%PROGRAMFILES%\psqlODBC\1600\bin\pgxalib.dll]- [targetUID: 00000000-00007100] "pgenlista.dll" has type "PE32+ executable (DLL) (GUI)

Creates new processes

Source API Call

Relevance 8/10

MITRE ATT&CK Native API T1106

Details "msiexec.exe" is creating a new process (Name: "C:\Windows\System32\MsiExec.exe")

Calls an API typically used to set the date and time of the file

Source API Call

Relevance 2/10

MITRE ATT&CK Timestomp T1070.006

Details "msiexec.exe" called "SetFileTime" on file C:\Windows\Installer\10e58f.msi (UID: 00000000-00007100) "msiexec.exe" called "SetFileTime" on file C:\Program Files\psqlODBC\1600\bin\libcrypto-3-x64.dll (UID: 00000000-00007100) "msiexec.exe" called "SetFileTime" on file C:\Program Files\psqlODBC\1600\bin\libiconv-2.dll (UID: 00000000-00007100) "msiexec.exe" called "SetFileTime" on file C:\Program Files\psqlODBC\1600\bin\libintl-9.dll (UID: 00000000-00007100) "msiexec.exe" called "SetFileTime" on file C:\Program Files\psqlODBC\1600\bin\libpq.dll (UID: 00000000-00007100) "msiexec.exe" called "SetFileTime" on file C:\Program Files\psqlODBC\1600\bin\libssl-3-x64.dll (UID: 00000000-00007100) "msiexec.exe" called "SetFileTime" on file C:\Program Files\psqlODBC\1600\bin\libwinpthread-1.dll (UID: 00000000-00007100) "msiexec.exe" called "SetFileTime" on file C:\Program Files\psqlODBC\1600\bin\msvcp140.dll (UID: 00000000-00007100) "msiexec.exe" called "SetFileTime" on file C:\Program Files\psqlODBC\1600\bin\pgenlist.dll (UID: 00000000-00007100) "msiexec.exe" called "SetFileTime" on file C:\Program Files\psqlODBC\1600\bin\pgenlist.pdb (UID: 00000000-00007100) "msiexec.exe" called "SetFileTime" on file C:\Program Files\psqlODBC\1600\bin\pgenlista.dll (UID: 00000000-00007100) "msiexec.exe" called "SetFileTime" on file C:\Program

Writes a PE file header to disc

Source API Call

Relevance 10/10

MITRE ATT&CK Ingress Tool Transfer T1105

Details "msiexec.exe" wrote 32499 bytes starting with PE header signature to file "C:\Program Files\psqlODBC\1600\bin\libcrypto-3-x64.dll": 4d5aff0003000000040000000ffff0000ff000000000000004000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000100000e1fff0e00ff09ff21ff014cff2154686973207072 6f6772616d2063616e6e6f742062652072756e20696e20444f53206d6f64652e0d0d0a2400000000000000 ... "msiexec.exe" wrote 24307 bytes starting with PE header signature to file "C:\Program Files\psqlODBC\1600\bin\libiconv-2.dll": 4d5aff0003000000040000000ffff0000ff000000000000004000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000ff0000000e1fff0e00ff09ff21ff014cff2154686973207072 6f6772616d2063616e6e6f742062652072756e20696e20444f53206d6f64652e0d0d0a2400000000000000 ... "msiexec.exe" wrote 8202 bytes starting with PE header signature to file "C:\Program Files\psqlODBC\1600\bin\libintl-9.dll": 4d5aff0003000000040000000ffff0000ff000000000000004000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000ff0000000e1fff0e00ff09ff21ff014cff2154686973207072 6f6772616d2063616e6e6f742062652072756e20696e20444f53206d6f64

Drops executable files

Source Binary File

Relevance 10/10

MITRE ATT&CK Ingress Tool Transfer T1105

Details "libcrypto-3-x64.dll" has type "PE32+ executable (DLL) (GUI) x86-64 for MS Windows"- Location: [%PROGRAMFILES%\psqlODBC\1600\bin\libcrypto-3-x64.dll]- [targetUID: 00000000-00007100] "libiconv-2.dll" has type "PE32+ executable (DLL) (console) x86-64 for MS Windows"- Location: [%PROGRAMFILES%\psqlODBC\1600\bin\libiconv-2.dll]- [targetUID: 00000000-00007100] "libssl-3-x64.dll" has type "PE32+ executable (DLL) (GUI) x86-64 for MS Windows"- Location: [%PROGRAMFILES%\psqlODBC\1600\bin\libssl-3-x64.dll]- [targetUID: 00000000-00007100] "msvcp140.dll" has type "PE32+ executable (DLL) (console) x86-64 for MS Windows"- Location: [%PROGRAMFILES%\psqlODBC\1600\bin\msvcp140.dll]- [targetUID: 00000000-00007100] "psqlodbc35w.dll" has type "PE32+ executable (DLL) (GUI) x86-64 for MS Windows"- Location: [%PROGRAMFILES%\psqlODBC\1600\bin\psqlodbc35w.dll]- [targetUID: 00000000-00007100] "psqlodbc30a.dll" has type "PE32+ executable (DLL) (GUI) x86-64 for MS Windows"- Location: [%PROGRAMFILES%\psqlODBC\1600\bin\psqlodbc30a.dll]- [targetUID: 00000000-00007100] "libintl-9.dll" has type "PE32+ executable (DLL) (console) x86-64 for MS Windows"- Location: [%PROGRAMFILES%\psqlODBC\1600\bin\libintl-9.dll]- [targetUID: 00000000-00007100] "libpq.dll" has type "PE32+ executable (DLL) (console) x86-64 for MS Windows"- Location: [%PROGRAMFILES%\psqlODBC\1600\bin\libpq.dll]-

Contains ability to modify thread functionality - possible hijack (API string)

Source File/Memory

Relevance 1/10

MITRE ATT&CK Thread Execution Hijacking T1055.003

Details Found reference to API "OpenThreadToken" (Indicator: "OpenThread"; Source: "00000000-00007100.00000002.72887.D288A000.00000002.mdmp")

Uses a Windows Living Off The Land Binaries (LOL bins)

Source Monitored Target

Relevance 3/10

Details Process "%WINDIR%\system32\msiexec.exe" launched with commandline "/V" (UID: 00000000-00007100) Process "%WINDIR%\System32\MsiExec.exe" launched with commandline "-Embedding F2B06C6509E020A304EBEA0E5E4D91F4" (UID: 00000000-00000752)

Tries to save executable or command in registry

Source Registry Access

Relevance 7/10

MITRE ATT&CK Boot or Logon Autostart Execution T1547

Details "msiexec.exe" (Access type: "SETVAL"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INSTALLER\USERDATA\S-1-5-18\PRODUCTS\8F07C821C47E7E943B1FB0C8CAA14F5C\INSTALLPROPERTIES"; Key: "MODIFYPATH"; Value: "MsiExec.exe /I{128C70F8-E74C-49E7-B3F1-0B8CAC1AF4C5}") "msiexec.exe" (Access type: "SETVAL"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INSTALLER\USERDATA\S-1-5-18\PRODUCTS\8F07C821C47E7E943B1FB0C8CAA14F5C\INSTALLPROPERTIES"; Key: "UNINSTALLSTRING"; Value: "MsiExec.exe /I{128C70F8-E74C-49E7-B3F1-0B8CAC1AF4C5}") "msiexec.exe" (Access type: "SETVAL"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL\{128C70F8-E74C-49E7-B3F1-0B8CAC1AF4C5}"; Key: "MODIFYPATH"; Value: "MsiExec.exe /I{128C70F8-E74C-49E7-B3F1-0B8CAC1AF4C5}") "msiexec.exe" (Access type: "SETVAL"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\UNINSTALL\{128C70F8-E74C-49E7-B3F1-0B8CAC1AF4C5}"; Key: "UNINSTALLSTRING"; Value: "MsiExec.exe /I{128C70F8-E74C-49E7-B3F1-0B8CAC1AF4C5}")

Looks up many procedures within the same disassembly stream (often used to hide usage)

Source Hybrid Analysis Technology

Relevance 10/10

MITRE ATT&CK T1027.007

Details Found 33 calls to GetProcAddress@KERNEL32.dll at 22779-2329-0000000180036664

Queries the installation properties of user installed products

Source Registry Access

Relevance 10/10

Details "msiexec.exe" (Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INSTALLER\USERDATA\S-1-5-18\PRODUCTS\8F07C821C47E7E943B1FB0C8CAA14F5C\INSTALLPROPERTIES") "msiexec.exe" (Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INSTALLER\USERDATA\S-1-5-18\PRODUCTS\8F07C821C47E7E943B1FB0C8CAA14F5C\INSTALLPROPERTIES"; Key: "AUTHORIZEDCDFPREFIX") "msiexec.exe" (Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INSTALLER\USERDATA\S-1-5-18\PRODUCTS\8F07C821C47E7E943B1FB0C8CAA14F5C\INSTALLPROPERTIES"; Key: "COMMENTS") "msiexec.exe" (Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INSTALLER\USERDATA\S-1-5-18\PRODUCTS\8F07C821C47E7E943B1FB0C8CAA14F5C\INSTALLPROPERTIES"; Key: "CONTACT") "msiexec.exe" (Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INSTALLER\USERDATA\S-1-5-18\PRODUCTS\8F07C821C47E7E943B1FB0C8CAA14F5C\INSTALLPROPERTIES"; Key: "DISPLAYVERSION") "msiexec.exe" (Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INSTALLER\USERDATA\S-1-5-

Contains ability to retrieve information about the current system

Source Hybrid Analysis Technology

Relevance 4/10

MITRE ATT&CK System Information Discovery T1082

Details GetSystemInfo@KERNEL32.dll at 22779-2752-0000000180004DE00

Calls an API typically used to query local/system time as file time

Source API Call

Relevance 3/10

MITRE ATT&CK Timestomp T1070.006

Details "msiexec.exe" called "FileTimeToLocalFileTime" with parameter 00f91c1b33e8d901 & 00f91c1b33e8d901 (UID: 00000000-00000728)
"msiexec.exe" called "FileTimeToLocalFileTime" with parameter 00f91c1b33e8d901 & 00f91c1b33e8d901 (UID: 00000000-00007100)

Contains ability to retrieve a module handle

Source Hybrid Analysis Technology

Relevance 5/10

MITRE ATT&CK System Information Discovery T1082

Details GetModuleHandleExW@KERNEL32.dll at 22779-1812-0000000180019762 GetModuleHandleExW@KERNEL32.dll at 22779-1814-00000001800197D5 GetModuleHandleExW@KERNEL32.dll at 22779-1815-0000000180019833 GetModuleHandleW@KERNEL32.dll at 22779-2750-0000000180004DD64

Contains ability to query CPU information

Source Hybrid Analysis Technology

Relevance 10/10

MITRE ATT&CK System Information Discovery T1082

Details cpuid at 22779-25-0000000018004D678 cpuid at 44522-16-0000000018000C250

Contains ability to retrieve the fully qualified path of module

Source Hybrid Analysis Technology

Relevance 5/10

MITRE ATT&CK Native API T1106

Details GetModuleFileNameW@KERNEL32.dll at 44522-166-00000001800050B0

Dropped file has high entropy (likely encrypted/compressed content)

Source Binary File

Relevance 5/10

MITRE ATT&CK Obfuscated Files or Information T1027

Details Dropped file "%WINDIR%\Installer\10e58f.msi" has high entropy 7.992882208843307 Dropped file "%WINDIR%\Installer\10e591.msi" has high entropy 7.992882208843307

Deletes registry keys

Source Registry Access

Relevance 3/10

MITRE ATT&CK Indicator Removal on Host T1070

Details "msiexec.exe" (Access type: "DELETEVAL"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INSTALLER\FOLDERS"; Key: "C:\CONFIG.MSI\"; Value: "") "msiexec.exe" (Access type: "DELETEVAL"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INSTALLER\ROLLBACK\SCRIPTS"; Key: "C:\CONFIG.MSI\10E590.RBS"; Value: "") "msiexec.exe" (Access type: "DELETEVAL"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INSTALLER\ROLLBACK\SCRIPTS"; Key: "C:\CONFIG.MSI\10E590.RBSLOW"; Value: "") "msiexec.exe" (Access type: "DELETEVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\RESTARTMANAGER\SESSION0000"; Key: "SEQUENCE"; Value:

"") "msiexec.exe" (Access type: "DELETEVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\RESTARTMANAGER\SESSION0000"; Key: "SESSIONHASH"; Value: "") "msiexec.exe" (Access type: "DELETEVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\RESTARTMANAGER\SESSION0000"; Key: "OWNER"; Value: "")

Writes registry keys

Source Registry Access

Relevance 3/10

MITRE ATT&CK Modify Registry T1112

Details 18\COMPONENTS\5B91A9C56C7D4BB4BBCB882C6AA7950B"; Key: "8F07C821C47E7E943B1FB0C8CAA14F5C"; Value: "%PROGRAMFILES%\psqlODBC\1600\bin\libpq.dll") "msiexec.exe" (Access type: "SETVAL"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INSTALLER\USERDATA\S-1-5-18\COMPONENTS\14C6A121F8B2D364AB48B63F761024A8"; Key: "8F07C821C47E7E943B1FB0C8CAA14F5C"; Value: "%PROGRAMFILES%\psqlODBC\1600\bin\pgxalib.dll") "msiexec.exe" (Access type: "SETVAL"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INSTALLER\FOLDERS"; Key: "C:\PROGRAM FILES\PSQLODBC\1600\BIN\"; Value: "0000") "msiexec.exe" (Access type: "SETVAL"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INSTALLER\FOLDERS"; Key: "C:\PROGRAM FILES\PSQLODBC\1600\"; Value: "0000") "msiexec.exe" (Access type: "SETVAL"; Path: "HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INSTALLER\FOLDERS"; Key: "C:\PROGRAM FILES\PSQLODBC\"; Value: "0000") "msiexec.exe" (Access type: "SETVAL"; Path: "HKLM\SOFTWARE\PSQLODBC_X64"; Key: "VERSION"; Value: "16.00.0000") "msiexec.exe" (Access type: "SETVAL"; Path: "HKLM\SOFTWARE\ODBC\ODBCINST.INI\POSTGRESQL ANSI";

Marks file for deletion

Source API Call

Relevance 10/10

MITRE ATT&CK File Deletion T1070.004

Details "msiexec.exe" marked "C:\Config.Msi\MSIF4E2.tmp" for deletion "msiexec.exe" marked "C:\Windows\Installer\10e591.msi" for deletion "msiexec.exe" marked "C:\Windows\Installer\MSIF261.tmp" for deletion "msiexec.exe" marked "C:\Config.Msi\MSIFCF2.tmp" for deletion "msiexec.exe" marked "C:\Config.Msi\10e590.rbs" for deletion "msiexec.exe" marked "C:\Windows\Installer\10e58f.msi" for deletion "msiexec.exe" marked "C:\Windows\Installer\inprogressinstallinfo.ipi" for deletion

Opens file with deletion access rights

Source API Call

Relevance 7/10

MITRE ATT&CK File Deletion T1070.004

Details	"msiexec.exe" opened "C:\Config.Msi\MSIF4E2.tmp" with delete access "msiexec.exe" opened "C:\Windows\Installer\inprogressinstallinfo.ipi" with delete access

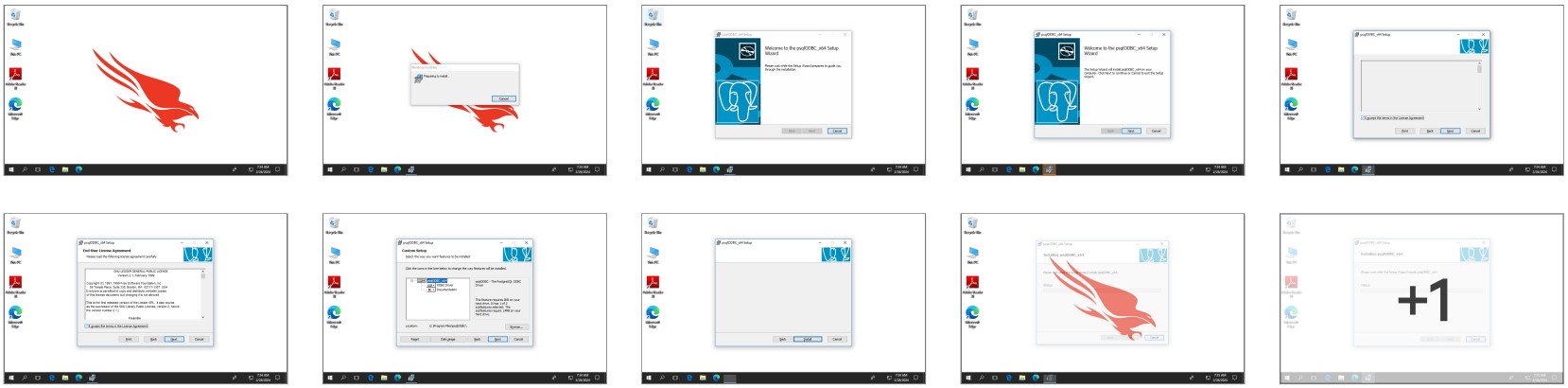
Informative 128

Process details

- msiexec.exe PID 728
- msiexec.exe PID 7100
  - MsiExec.exe PID 752

Screenshots

Show all Off



Extracted strings

Download extracted strings

vcruntime140.dll.2765944609	40
pgenlista.dll	1
pgenlist.dll	1
psqlodbc_x64.msi	60
msiexec.exe	215
msvcp140.dll.1359509395	1617
ngen.log	343
ODBCINST.INI	1
screen_10.png	2
screen_5.png	1

Extracted files

No verdict 20