






T1218.008 — DLL execution using ODBCCONF.exe

Harjot Shah Singh · Follow
2 min read · May 8, 2023

 -- 

What is ODBCConf.exe?

ODBCConf.exe is a Microsoft Windows utility that is used to manage Open Database Connectivity (ODBC) data sources. ODBCConf.exe allows you to configure and manage ODBC drivers and data sources on your computer. ODBC is a standard API (Application Programming Interface) for accessing data from different databases using SQL (Structured Query Language).

ODBCConf.exe is typically located in the “System32” folder of a Windows installation, and can be accessed from the Command Prompt or Run dialog box.

How threat actors can abuse ODBCconf.exe?

Threat actors can abuse ODBCConf.exe in a number of ways, including: Malware Persistence, Data Exfiltration, Credential Theft, Malicious Software Execution, etc.

This writing will cover how threat actors can execute malicious DLL using odbccong.exe binary.

Creating a DLL to execute calc.exe?

Following C++ code can be compiled using Visual Studio as a DLL and upon execution of the compiled DLL, it will spawn calc.exe.

```
#include <windows.h>

BOOL APIENTRY DllMain(HMODULE hModule, DWORD ul_reason_for_call, LPVOID lpReserved)
{
    switch (ul_reason_for_call)
    {
        case DLL_PROCESS_ATTACH:
            // Execute Calculator
            WinExec("calc.exe", SW_SHOW);
            break;
    }
}
```

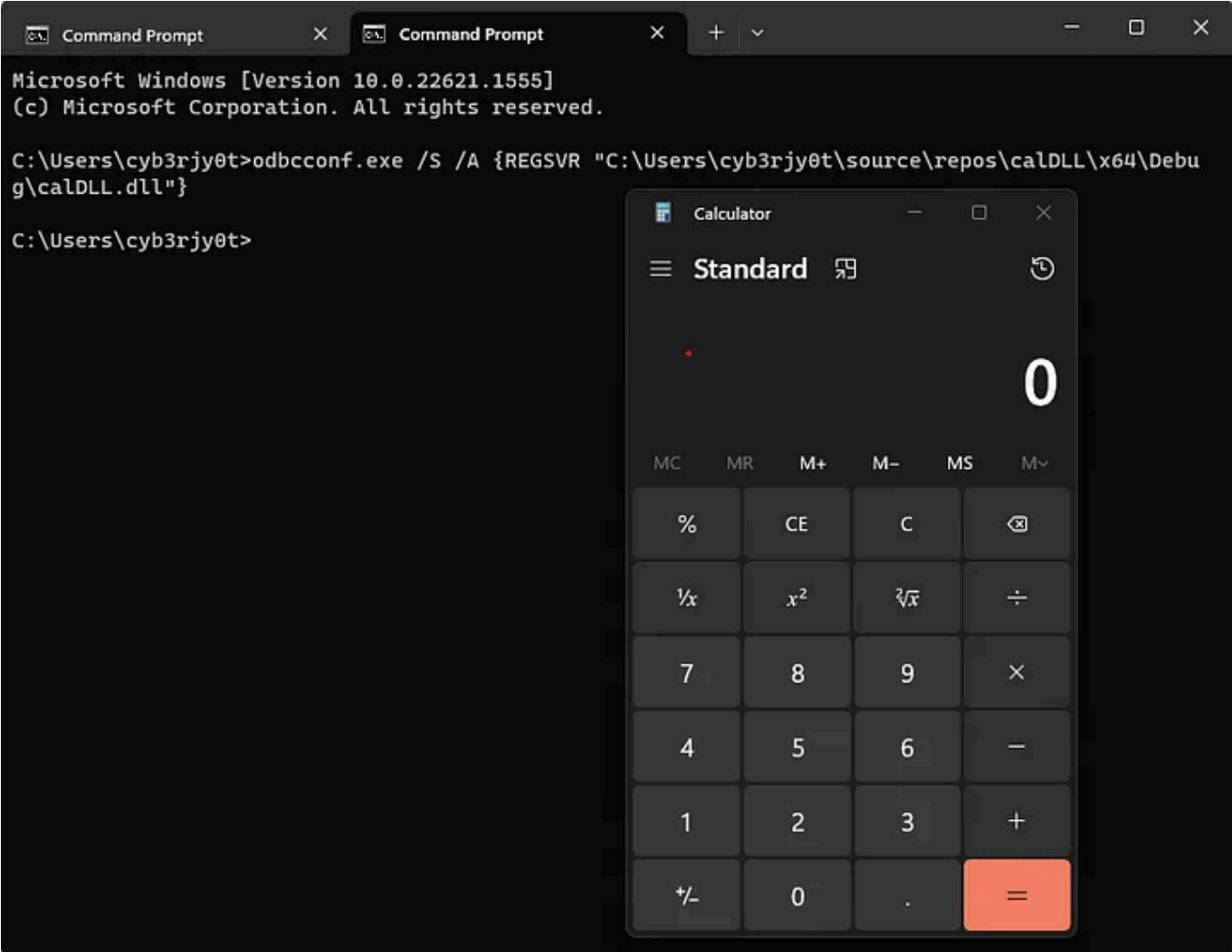
```
        return TRUE;
    }
```

The compiled DLL can be downloaded from github:

<https://github.com/cyb3rjy0t/CalcDLL>

Abusing ODBCCONF.exe to execute DLL

Upon execution of the command, following artifacts are generated:



@tim	agent.host	process.name	process.command_line	process.parent.command_line	process.parent	event.code	winlog.eve	winlog.eve	process	process.pid	event.provi
Apr 29, 2023 @ 17:42:32...	lab	calc.exe	calc.exe	odbcconf.exe /S /A (REGSVR "C:\Users\cyb3rjy0t\source\repos\calDLL\x64\Debug\calDLL.dll")	odbcconf.exe	1	Windows Calculator	CALC.EXE	12,232	38,712	Microsoft-Windows-Sysmon
Apr 29, 2023 @ 17:42:32...	lab	odbcconf.exe	odbcconf.exe /S /A (REGSVR "C:\Users\cyb3rjy0t\source\repos\calDLL\x64\Debug\calDLL.dll")	C:\WINDOWS\System32\cmd.exe	cmd.exe	1	ODBC Driver Configuration Program	odbcconf.exe	32,508	12,232	Microsoft-Windows-Sysmon

Detection

The possible detection after observing the Windows Sysmon logs

- Monitoring the process command line in event ID 1

```
event.code: 1 AND (process.name: "odbcconf.exe" OR original.file_name:"odbcconf.exe"
```



2. Monitoring Child Processes Spawned By ODBCCONF.exe

event.code: 1 AND parent.process.name: "odbcconf.exe"

3. Monitoring event ID 7 for suspicious DLLs loaded by ODBCCONF.exe

event.code: 7 AND process.name: "odbcconf.exe"

References

- <https://attack.mitre.org/techniques/T1218/008/>
- <https://dmcxblue.gitbook.io/red-team-notes-2-0/red-team-techniques/defense-evasion/t1218-signed-binary-proxy-execution/untitled-4>
- <https://learn.microsoft.com/en-us/sql/odbc/odbcconf-exe?view=sql-server-ver16>
- <https://redcanary.com/blog/raspberry-robin/>
- <https://chat.openai.com/>

Detection Engineering

Cybersecurity

Mitre Attack

Defense Evasion

Security Operations





Written by Harjot Shah Singh

Follow



0 Followers

Cyb3rjy0t