Process Injection Part III

Shellcode Generation • COM Injection • Kernel Bypass

Module Overview

3 theory sections • 6 injection techniques • Stardust PIC payloads • BYOVD PPL bypass • Practical exercise

THEORY & FUNDAMENTALS

01 Introduction

Module overview and prerequisites

02 Review: Process Injection Parts I & II

Techniques covered in the previous modules

03 Theory: Stardust Shellcode Template NEW

Writing position-independent shellcode in C++20

API hashing • compile-time string encryption • symbol<> helper • PIC architecture

04 Theory: Creating a Reverse Shell with Stardust NEW

Adapting standard C++ to position-independent shellcode

RESOLVE_API • LoadLibraryA • symbol strings • Winsock + cmd.exe

INJECTION TECHNIQUES

05 COMouflage: Surrogate Injection

DLL injection via Windows COM DLL Surrogate mechanism

HKCU registry • DllSurrogate • CoCreateInstance • svchost parent masquerading

06 Credential Provider DLL Hijacking

Persistent DLL execution on every Windows logon as SYSTEM

HKLM Credential Providers • COM InprocServer32 • LogonUI.exe • NT AUTHORITY\SYSTEM

07 Thread Name-Calling

Shellcode injection via thread description API without PROCESS_VM_WRITE

SetThreadDescription • GetThreadDescription APC • ZwQueueApcThreadEx2 • NonPagedPoolNx

08 Userland Write Primitive

Drop-in WriteProcessMemory replacement using thread names

SetThreadDescription • Special User APC • PEB+0x340 scratchpad • evasive remote write

09 Process Hollowing

Replace a suspended process image with a malicious PE

CREATE_SUSPENDED • NtUnmapViewOfSection • LoadPEImage • SetThreadContext RCX

10 Bonus: Injection into PPL Processes KERNEL BONUS

Bypass Protected Process Light via BYOVD kernel R/W

GDRV CVE-2018-19320 • EPROCESS walk • PS_PROTECTION byte • PPL deactivation

PRACTICE & APPLICATION

11 Hands-on Exercise

Build a Stardust-powered injector against a PPL process

Stardust reverse shell + evasive write or hollowing + optional BYOVD PPL bypass

12 Conclusions & Future Trends

Summary, detection landscape, and where injection research is heading