Module Structure

RPC FOR MALWARE DEVELOPMENT

ADVANCED · WINDOWS INTERNALS · 0X12 DARK DEV

THEORY

00 Introduction

Scope, ethical context, and RPC as a universal Windows attack surface.

01 What is RPC?

Client-server model, marshalling, NDR, protocol sequences & IDL file structure.

02 RPC Attack Surface

EDR evasion via proxy model, payload fragmentation & lateral movement primitives.

TECHNIQUES

T1 Inter-Process Communication

Basic ncalrpc message passing between a server and client over ALPC.

T2 RPC IPC from Remote Computer

TCP-based RPC (ncacn_ip_tcp) for cross-machine communication on port 4444.

T3 RPC Proxy Injection

DLL as RPC client inside legitimate process — server holds shellcode & executes.

T4 Inject DLL with RPC Server

Inverted model — DLL hosts the server; custom WriteProcessMemory breaks EDR chain.

T5 Main Process Malware Controller

Centralized ALPC orchestrator with distributed worker DLLs in trusted host processes.

→ Exercise

Challenge 1: Bidirectional message bus. Challenge 2: Full implant controller simulation.

■ Conclusions

RPC as a paradigm shift — compartmentalization, attribution confusion & resilience.