Modern Malware Internals and Analysis

### Phishing Email
- **Project.htm** downloaded to victim's machine
- User **double-clicks** project.chm

### Infection Chain
1. **Start hh.exe**
2. **Start injected browser_broker.exe**
3. **Establish network connections to C&C**

### Start.htm → 43ptpmyc.dll
- Executes .NET dll by applying technique similar to DotNetToJScript
- Usage of popular .NET deserialization gadget

### OfficeHTMLHelper.exe
- Instantiates class that can perform Anti-Debugging/Sandbox checks
- Overwrites .text section of ntdll.dll with clean copy to remove EDR hooks
- Extracts shellcode from .rsrc section hidden in multiple layers of compression, encoding, and encryption

### Shellcode Injection
1. Create instance of browser_broker.exe (used by Edge) in suspended state
2. Insert shellcode into process memory
3. Queue shellcode as user-mode APC
4. Resume thread
- This version of APC injection avoids EDR detection by running code before process can be hooked

### Detection & Analysis Challenges
- Matryoshka-style encapsulation delays analysis but does not increase difficulty
- Since solely the initial payload project.htm is written to the filesystem, which contains common JavaScript code, static detection is impractical

### Tooling:
- Static: IDA, dnSpy
- Dynamic: x64dbg, Cyberchef, hollows-hunter