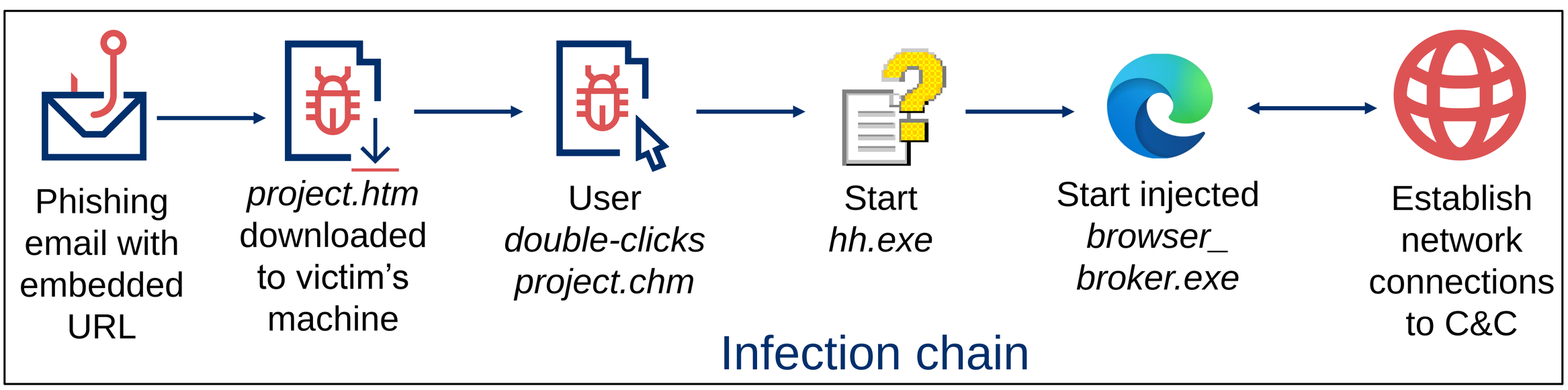
Tactical Defense Unit, WithSecure

Philipp Giersfeld, Catarina de Faria Cristas

Modern Malware Internals and Analysis



Infection chain

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

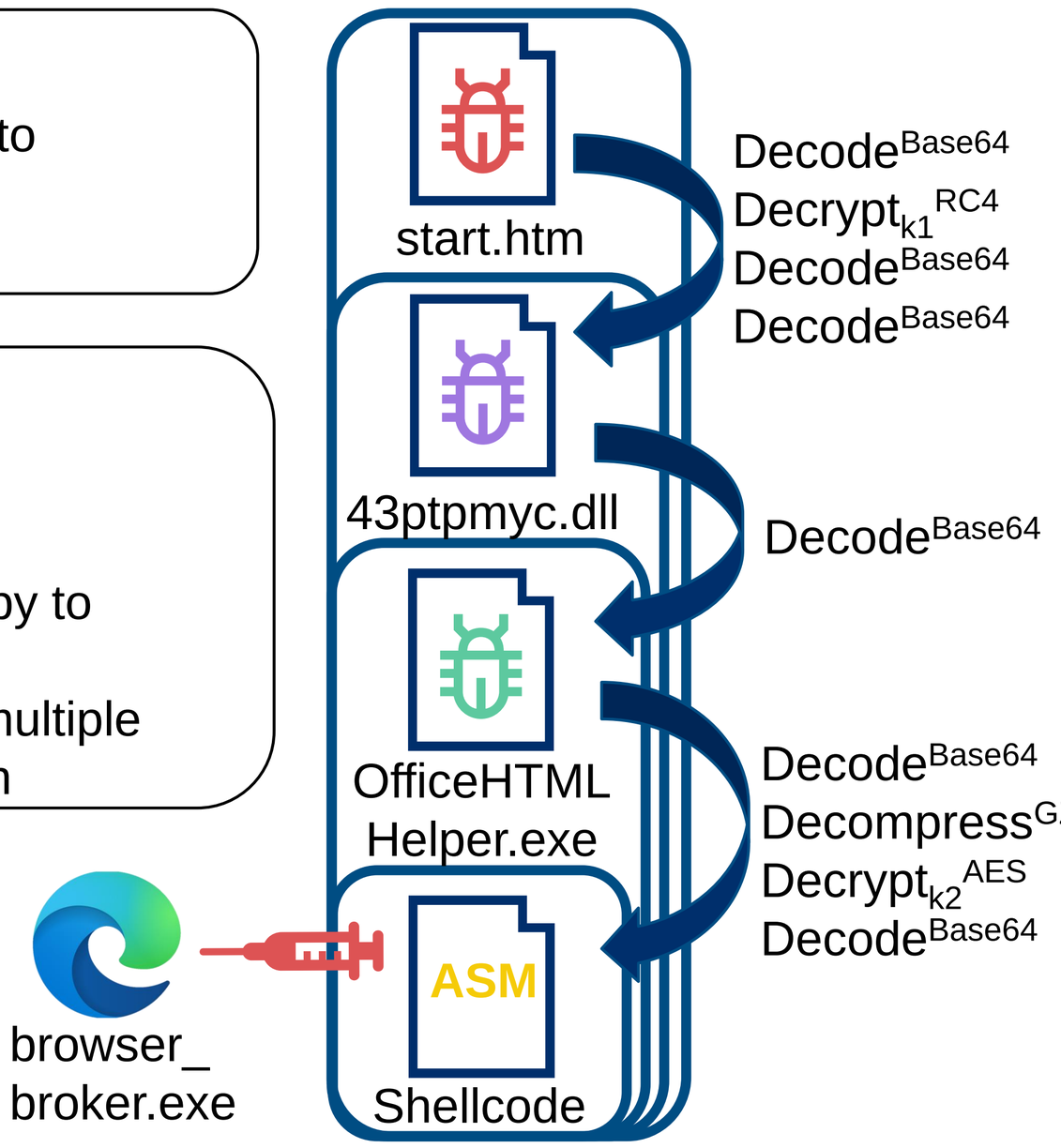
Shellcode injection

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




```
xor     ecx, ecx          ; Time
call    _time64           ; Microsoft VisualC 64bit universa
cmp     rax, 1642961490 ; Sun Jan 23 2022 18:11:30
jle     short loc_180051E78

call    cs:__imp_GetCurrentProcess
mov     rcx, rax          ; hProcess
xor     edx, edx          ; uExitCode
call    cs:TerminateProcess
```

Final DLL contains check to abort execution if system time is after 23.01.2022

Tooling:

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

WITH secure