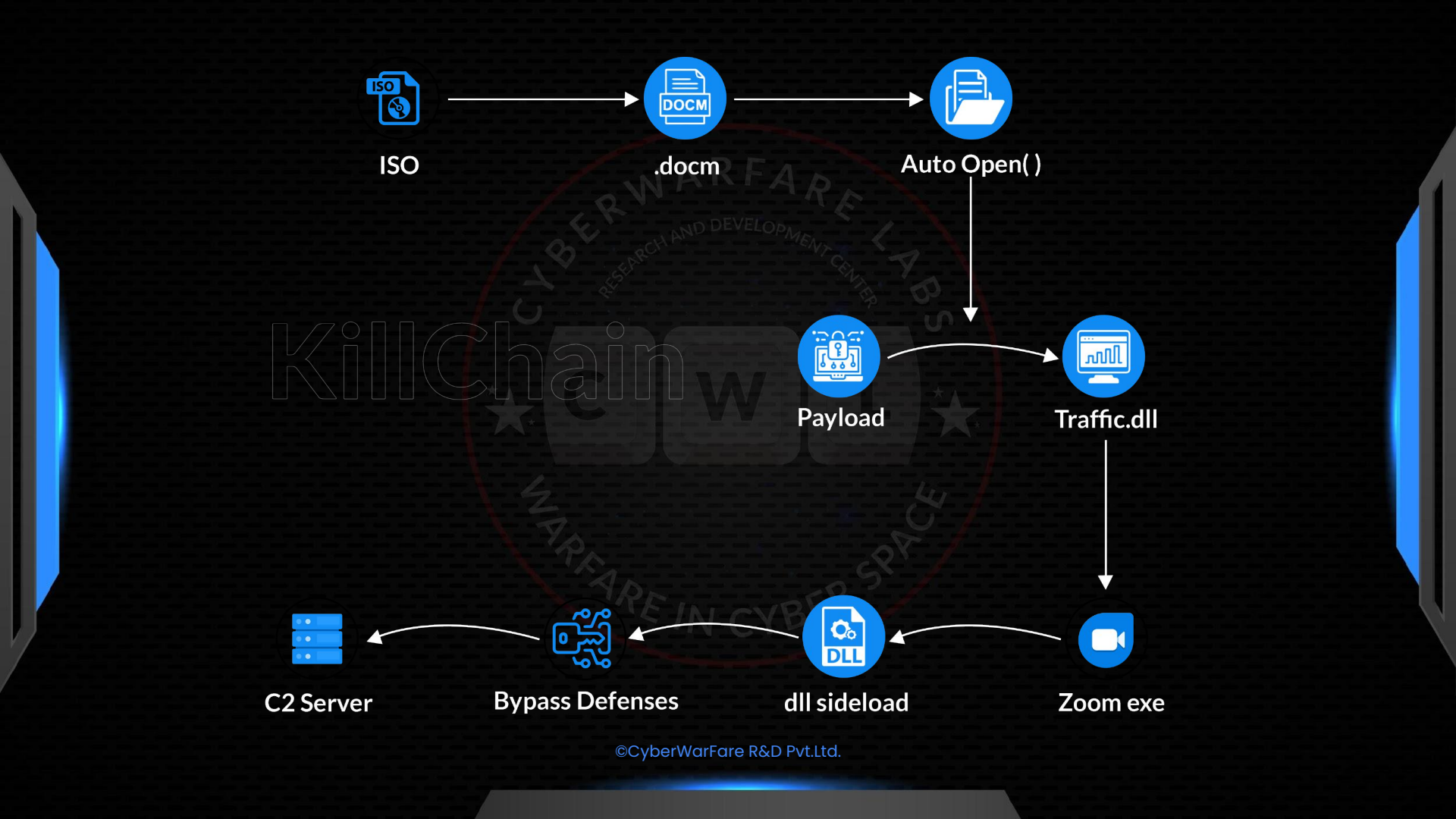
“Persistence in Zoom via DLL Hijacking & Bypassing Zoom's Anti-Tampering Library”

By: CyberWarFare Labs Team

Contents

- Kill Chain
- DLL (Dynamic Link Library)
- DLL Hijacking
- DLL Proxying
- Zoom’s Anti-tampering library
- Bypass anti-tampering


ISO
.docm
Auto Open( )
Payload
Traffic.dll
Zoom exe
dll sideload
Bypass Defenses
C2 Server
KillChain
CYBER WARFARE LABS
RESEARCH AND DEVELOPMENT CENTER
WARFARE IN CYBER SPACE
©CyberWarFare R&D Pvt.Ltd.

DLL (Dynamic Link Library)

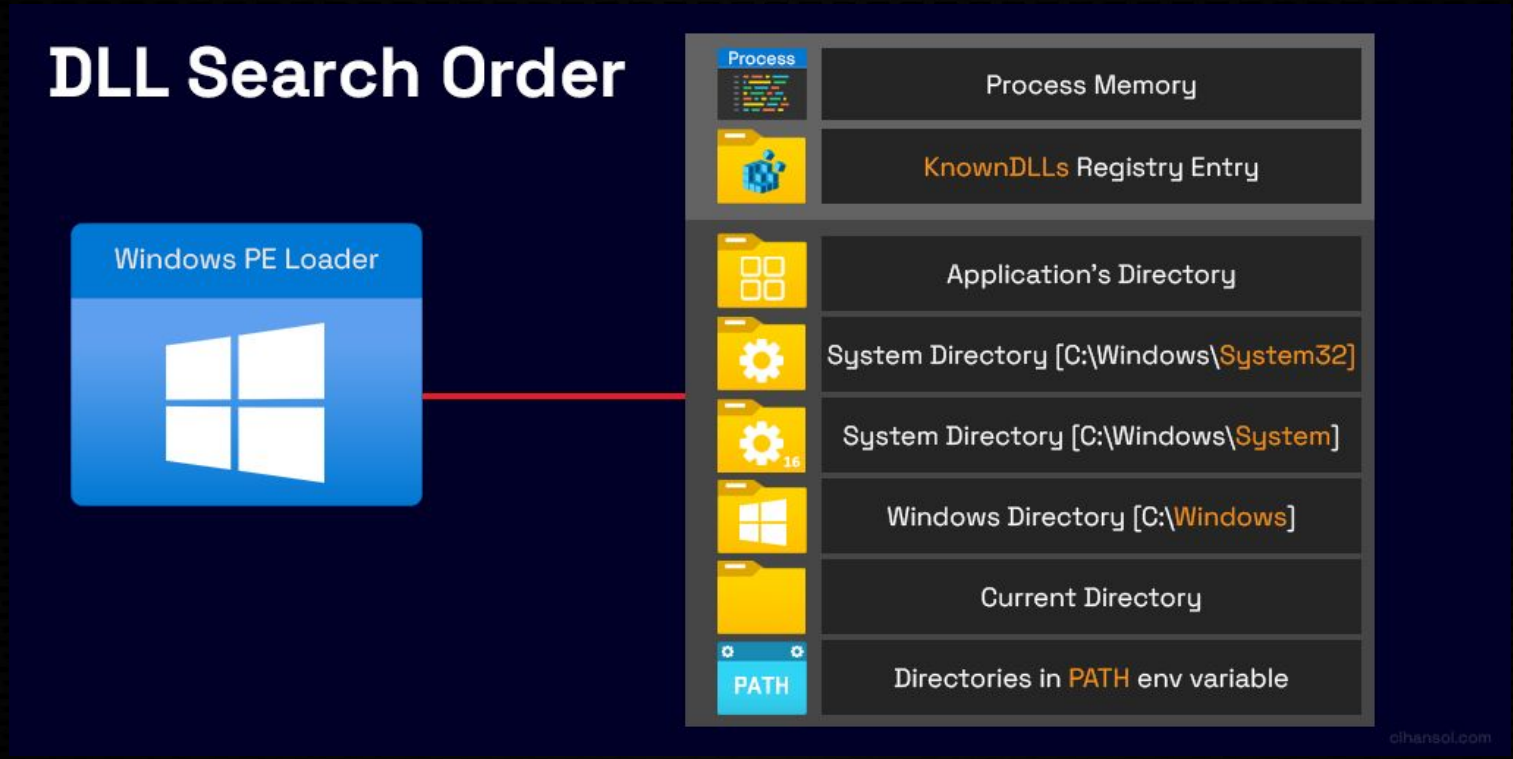
- DLLs are the shared libraries used in Windows OS
  - Allows multiple programs to use the same code
  - Extensively used by many system components, applications etc. in Windows OS

DLL Hijacking

- DLL hijacking is a technique that tricks a program into loading a malicious DLL instead of the intended legitimate DLL
  - Normally missing legitimate dll is replaced by malicious one in a location where application will search for it to execute arbitrary code
  - The malicious code run as a same privilege level as the victim application; sometimes leads to privilege escalation
  - T1574: Hijack Execution Flow

DLL Search Order Hijacking

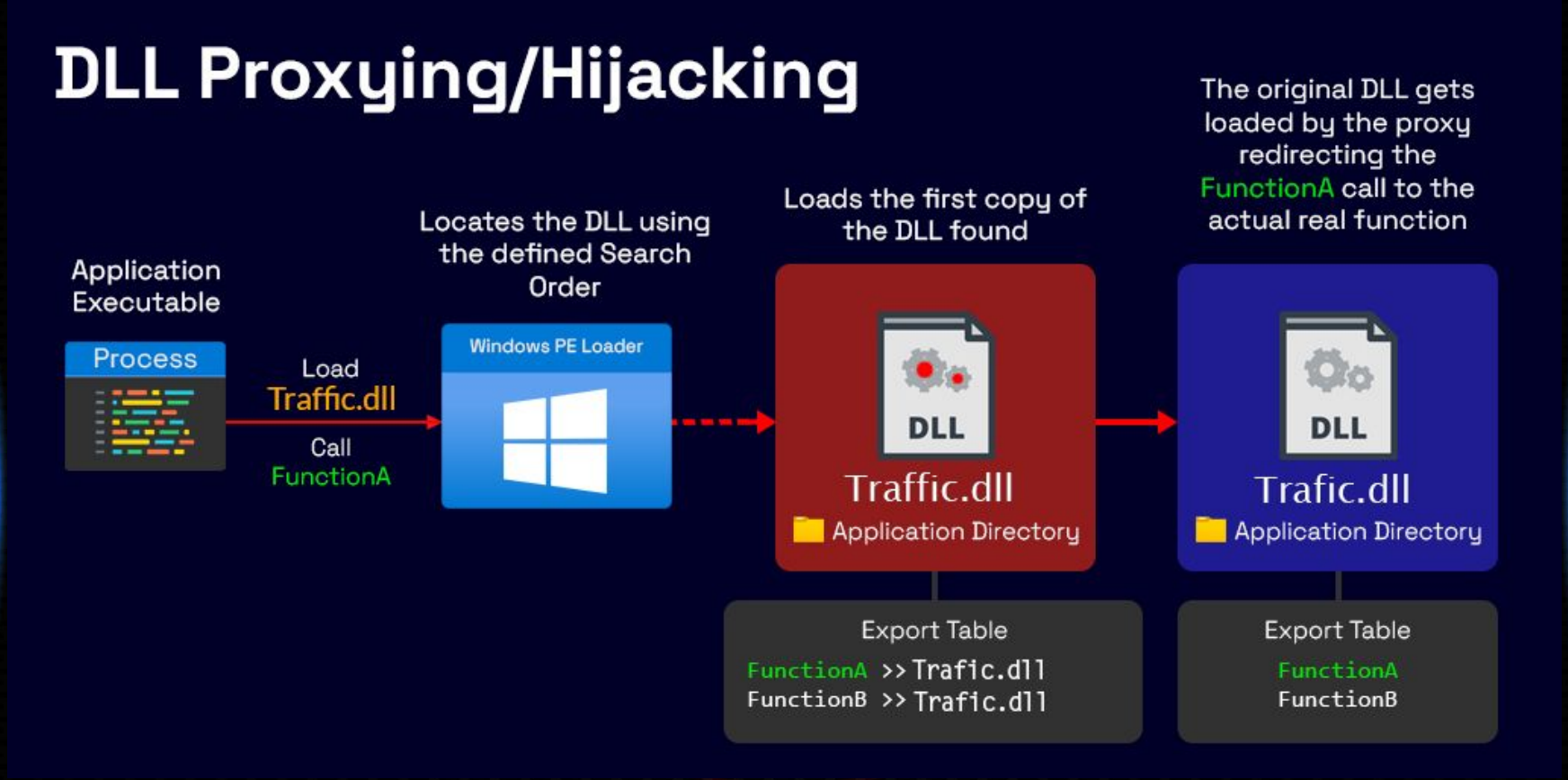
- Attacker hijacks the DLL search order mechanism of Windows Operating system
  - Malicious dll is placed in a directory before the actual directory containing the legitimate dll
  - Microsoft has default route for searching dll



DLL Search Order [2]

DLL Proxying

- Technique to load the malicious DLL while still maintaining the functionality of the legitimate DLL that the application depends on
  - DLL wrapper is used in this technique
  - Wrapper dll Intercepts a call made by the application and forward it to the legitimate dll



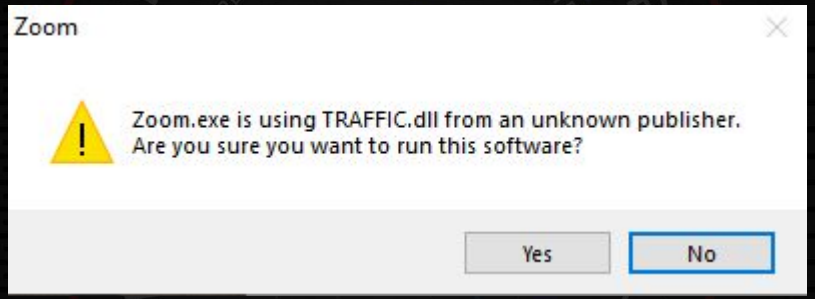
DLL Proxying [2]

Zoom's Anti-tampering Library

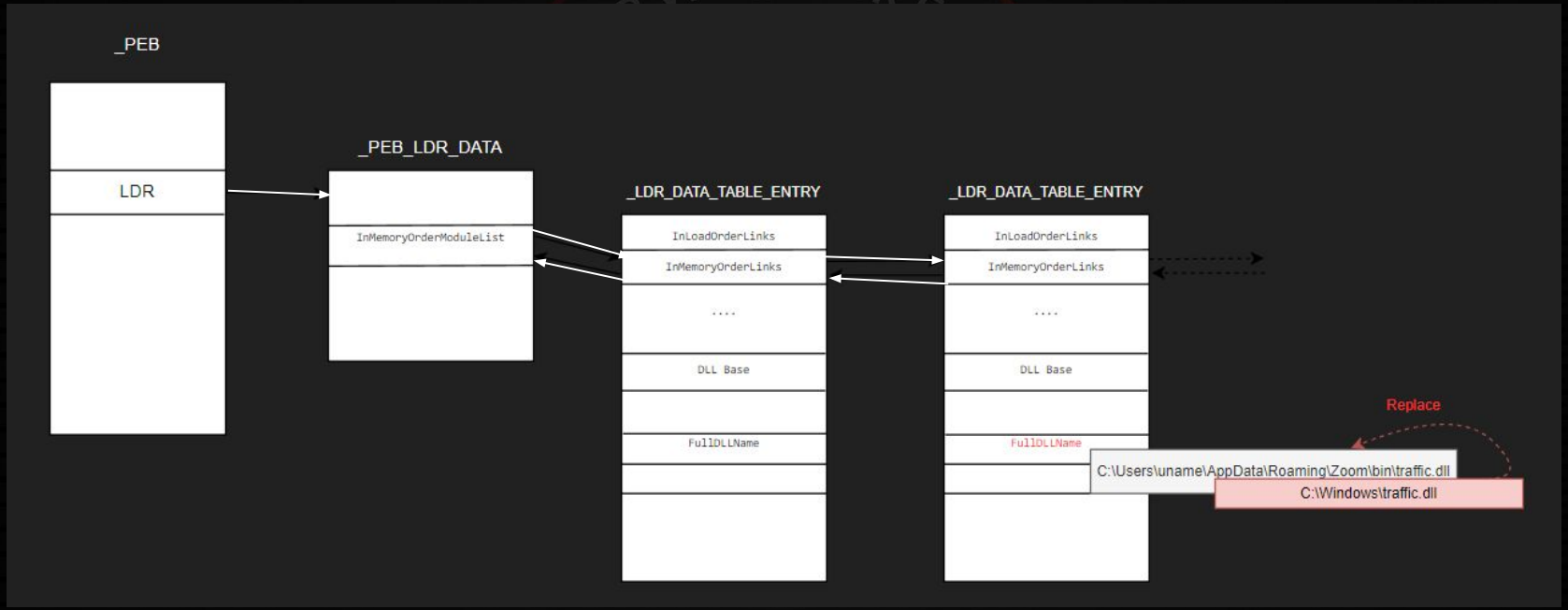
```
if ( sub_40C480(LOWORD(lpMem[0]) >> 1, (int)lpMem[1], (wint_t *)this + 4) )// checks if path is %appdata%/zoom/bin/ |
                                        // returns 1 if true
{

  if ( alloc_size_v27 )
  {
    if ( !*(_BYTE *)alloc_size_v27 )
      goto LABEL_43;
    v18 = alloc_size_v27[2];
  }
  else
  {
    v18 = 0;
  }
  v19 = is_dll_verified((WCHAR *)v11, v18, &v27);// checks if dll is verified or not
  goto LABEL_40;
```

Zoom's Anti-tampering Library



Bypass Anti-tampering library



https://www.cyberwarfare.live/trainings/stealthops-training

References

1. https://learn.microsoft.com/en-us/troubleshoot/windows-client/deployment/dynamic-link-library
2. https://cihansol.com/blog/index.php/2021/09/14/windows-dll-proxying-hijacking/