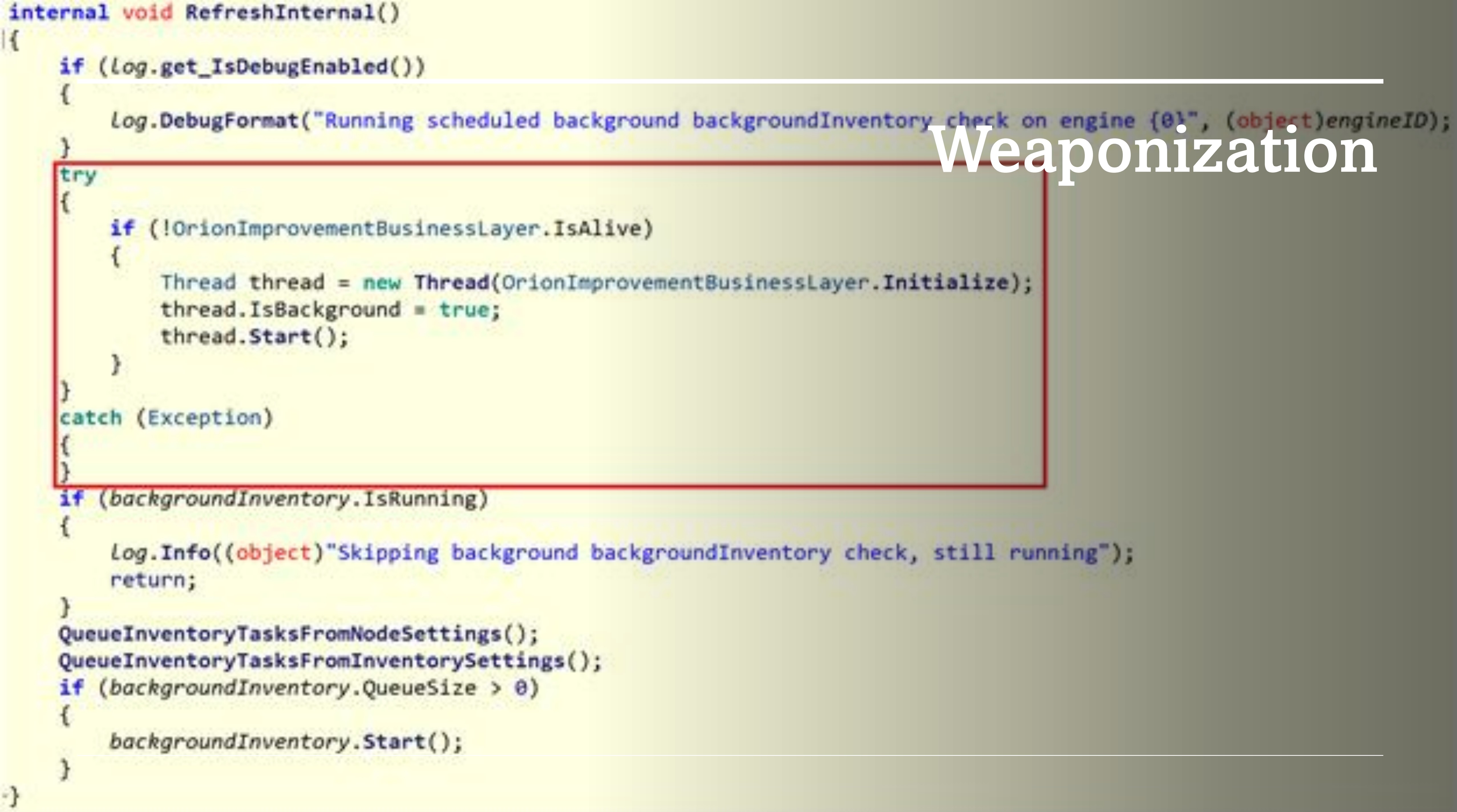
The Solar Winds Breach Case Study

The Exploit

Cyber Kill Chain Stage	Solar Winds Example
Reconnaissance	
Weaponization	Modified Sealed Software Code
Delivery	Routine Software Update
Exploitation	Trusted Network Monitoring Software
Installation	User Download and Deployment
Command & Control	Mimicked Communication Protocols
Actions on Objectives	Unknown (Espionage)

Weaponization



```
internal void RefreshInternal()
{
    if (Log.get_IsDebugEnabled())
    {
        Log.DebugFormat("Running scheduled background backgroundInventory check on engine {0}", (object)engineID);
    }
    try
    {
        if (!OrionImprovementBusinessLayer.IsAlive)
        {
            Thread thread = new Thread(OrionImprovementBusinessLayer.Initialize);
            thread.IsBackground = true;
            thread.Start();
        }
    }
    catch (Exception)
    {
    }
    if (backgroundInventory.IsRunning)
    {
        Log.Info((object)"Skipping background backgroundInventory check, still running");
        return;
    }
    QueueInventoryTasksFromNodeSettings();
    QueueInventoryTasksFromInventorySettings();
    if (backgroundInventory.QueueSize > 0)
    {
        backgroundInventory.Start();
    }
}
```

Installation – Further Reconnaissance

- It verifies that the process hosting the malicious DLL is named *solarwinds.businesslayerhost.exe*
- It checks that the last write-time of the malicious DLL is at least 12 to 14 days earlier
- It delays execution by random amounts of time
- It verifies that the domain name of the current device meets the following conditions:
    - The domain must not contain certain strings; the check for these strings is implemented via hashes, so at this time the domain names that are block-listed are unknown
    - The domain must not contain “solarwinds”
    - The domain must not match the regular expression *(?i)([^a-z]|^)(test)([^a-z]|$)*, or in simpler terms, it must not look like a test domain
- It checks that there are no running processes related to security-related software (e.g., *Windbg*, *Autoruns*, *Wireshark*)
- It checks that there are no drivers loaded from security-related software (e.g., *groundling32.sys*)
- It checks that the status of certain services belonging to security-related software meets certain conditions (e.g., *windefend*, *sense*, *cavp*)
- It checks that the host “api.solarwinds.com” resolves to an expected IP address

C2 Commands

- Idle
- Exit
- SetTime
- CollectSystemDescription
- UploadSystemDescription
- RunTask
- GetProcessByDescription
- KillTask
- GetFileSystemEntries
- WriteFile
- FileExists
- DeleteFile
- GetFileHash
- ReadRegistryValue
- SetRegistryValue
- DeleteRegistryValue
- GetRegistrySubKeyAndValueNames
- Reboot
- None

Mitigation

Cyber Kill Chain Stage	Solar Winds Example	Mitigation
Reconnaissance		
Weaponization	Modified Sealed Software Code	Secure Hashing
Delivery	Routine Software Update	
Exploitation	Trusted Network Monitoring Software	Risk Management Process
Installation	User Download and Deployment	
Command & Control	Mimicked Communication Protocols	
Actions on Objectives	Unknown (Espionage)	