Protecting End-Users from Supply Chain Attacks

The recent attack leveraging the SolarWinds supply chain have exposed significant flaws in how conventional security tools defend against advanced malware. This document provides key take-aways from the attacks, and details on how the Virsec Security Platform (VSP) can effectively stop these complex attacks at multiple stages.

Take-Aways from the SolarWinds Attack

The SolarWinds attack used the software supply chain to deliver malware that opened backdoor channels for attackers to exploit. Equally importantly, they also leveraged vulnerabilities in software workloads that enabled Remote Code Execution (RCE) to further exploit government and enterprise infrastructure. Key take-aways:

a. **Memory Injection Attacks are Lethal**: An advisory from DHS indicates that the main backdoor library needed an accompanying unsigned library C:\WINDOWS\SysWOW64\netsetupsvc.dll to also load into memory. This DLL assisted the backdoor library in both the weaponization and the exploitation phases of the attack.

   VSP will automatically suspend any process or script in which any unsigned or unauthorized code attempts to run. VSP will also suspend any process triggered from an unauthorized app or script even if this code is perfectly legal elsewhere.

b. **RCE Vulnerabilities Can Be Disastrous**: Conventional security tools cannot detect attacks that generate attacker-influenced code directly in memory. Each week, hundreds of new RCE vulnerabilities are reported in the National Vulnerability Database (NVD), making it impractical to instantly patch these vulnerabilities or create signatures against all exploits.

   Virsec's Application-Aware technology is unique in detecting and stopping RCE attacks during runtime, without prior knowledge.

c. **Real-Time Protection is Mandatory**: Most security tools wait far too long in the attack kill - initial infiltration, persistence, weaponization, and exploitation stages, before detecting threats and taking action. This extensive dwell time dramatically increases the risk of damage.

   VSP patented technology can abort attacks at the initial infiltration stage in real time, preventing subsequent attack stages.

d. **Threat Feed Based Solutions are Ineffective**: Bad actors generate almost 350K new malware every day. It is almost impossible for Security Controls such as EDR that use AI/ ML engines to keep up. AI/ ML engines extract models from known malware but there is no reason to believe that these tools see everything or that malware variants will repeat. These approaches are porous at best, and new sophisticated malware can operate unnoticed.

   Virsec requires no prior knowledge, signatures, or learning to stop advanced malware the first time.

e. **Precision is Key to Timely Protection**: EDR solutions wait until a threshold of "potentially malicious" activity is reached, which in the case of a sophisticated attack may be never.

   VSP uses precise inline techniques to detect and stop attacks, the instant attacker-provided code begins to execute.

f. **Firestorm of RCE Vulnerabilities Headed to your Web Facing Apps**: If you have web facing software applications, the risk posed by not protecting your infrastructure with Virsec's Application Aware Workload Protection cybersecurity technology is simply too high.

Following is a more detailed explanation of how Virsec's Application-Aware Workload Protection Controls are purpose-built to protect against sophisticated supply chain attacks. A more detailed analysis of the end-to-end SolarWinds attack can be found here.

Virsec Security Platform (VSP)

VSP patented technology is delivered via the following three application-aware components

a. **VSP Memory**: leverages in-memory instrumentation to detect and protect when a workload starts executing attacker provided shell code

b. **VSP Web**: leverages in-memory instrumentation to detect and protect when a workload starts executing attacker provided byte code

c. **VSP Host**: leverages file integrity capabilities to prevent even single instructions from any unauthorized executables, libraries, and scripts from executing

Unlike EDR and other Security Controls, the VSP source of truth is the application's code itself. Once a developer delivers an application, the Virsec source of truth **never** changes unlike other security controls that depend on a moving target of threat feeds.

Stages in the SolarWinds Attack

The attack on end-users of SolarWinds proceeded along the following two stages:

1. **Backdoor Deployment**: Via malware backdoor delivered through SolarWinds updates. This allowed the attackers to persist in the victim enterprise and conduct malicious activities at will.
2. **Lateral Movement**: Spreading the malware to all "neighbors."

Protecting Your Infrastructure from Corrupted SolarWinds Updates

The diagram below details the events in the SolarWinds attack, and where Virsec protects versus EDRs. Virsec's protection technology can protect your SolarWinds server from executing unauthorized apps and scripts and from loading unsigned and inappropriate libraries. Even if these apps are perfectly legitimate on another server.

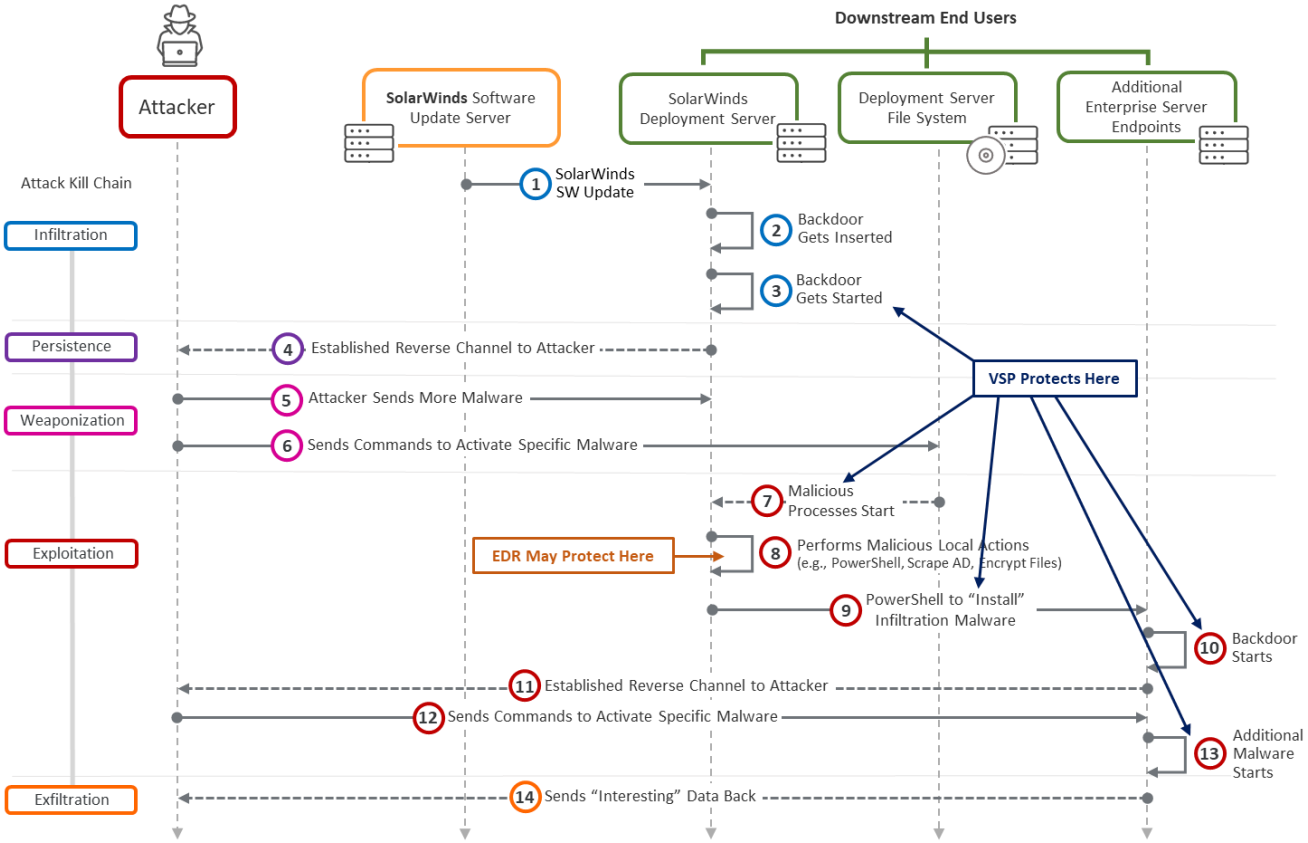

Figure 1: Virsec protection in the SolarWinds Supply Chain attacks

Protecting Your Infrastructure from RCE Vulnerabilities

Please refer to the chain of events shown in the sequence diagram below. Virsec's Application Aware Workload Protection technology can protect your web facing workloads from being attacked EVEN when it is not possible to patch it continuously and remove vulnerabilities that can result in remote code execution (RCE).

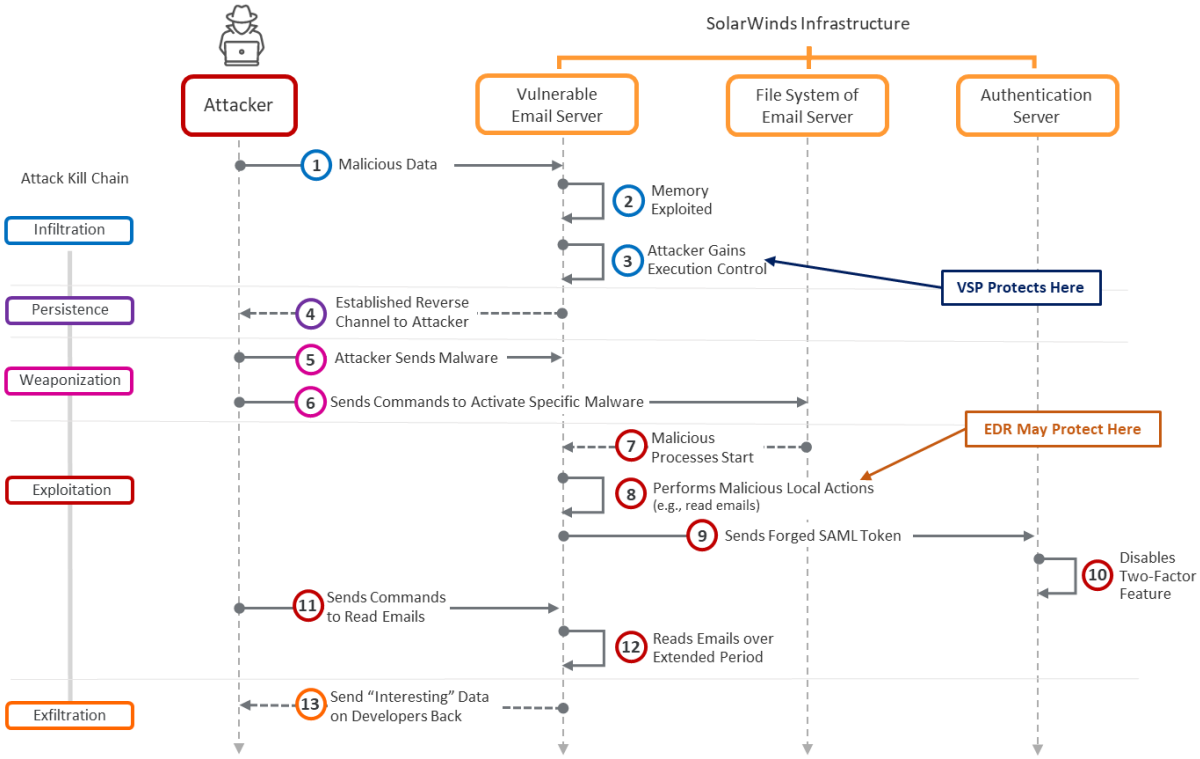

Figure 2: Virsec protection against RCE vulnerabilities

Conclusions

The Virsec Security Platform (VSP) is designed to protect enterprises from such sophisticated RCE or Supply Chain attacks on on-premises, cloud, hybrid, or container-based workloads. For more details, please contact us at www.virsec.com