Protecting Enterprise Infrastructure from RCE 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. **RCE Vulnerabilities Can Be Disastrous:** One report claims a critical memory deserialization vulnerability (CVE-2020-0688) in SolarWinds Exchange Server provided the entry point for attackers to infiltrate SolarWinds. Another report attributes the entry point to a critical command injection vulnerability (CVE-2020-4066) in the SolarWinds VMware identity management software. To make matters worse, each week, an avalanche of new RCE vulnerabilities is reported into the National Vulnerability Database (NVD).

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

b. **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.

c. **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.

d. **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.

e. **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 stages:

1. **Initial Infiltration**: Via exploitation of the email server and subsequent compromise of the authentication service. This allowed the attackers to persist in the victim enterprise and go on to examine email and develop a profile on the developers they needed to target
2. **Reconnaissance**: Launching of a spear phishing campaign that targeted the developers of interest
3. **Spear Phishing**: Infecting the machines of the targeted developers
4. **Weaponization or Insertion of Backdoor**: Manipulating the build system to insert their backdoor

Using VSP to Block at the First Stage – Initial Infiltration

The diagram below details the events in the SolarWinds attack, and where Virsec protects versus EDRs. 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 RCE vulnerabilities.

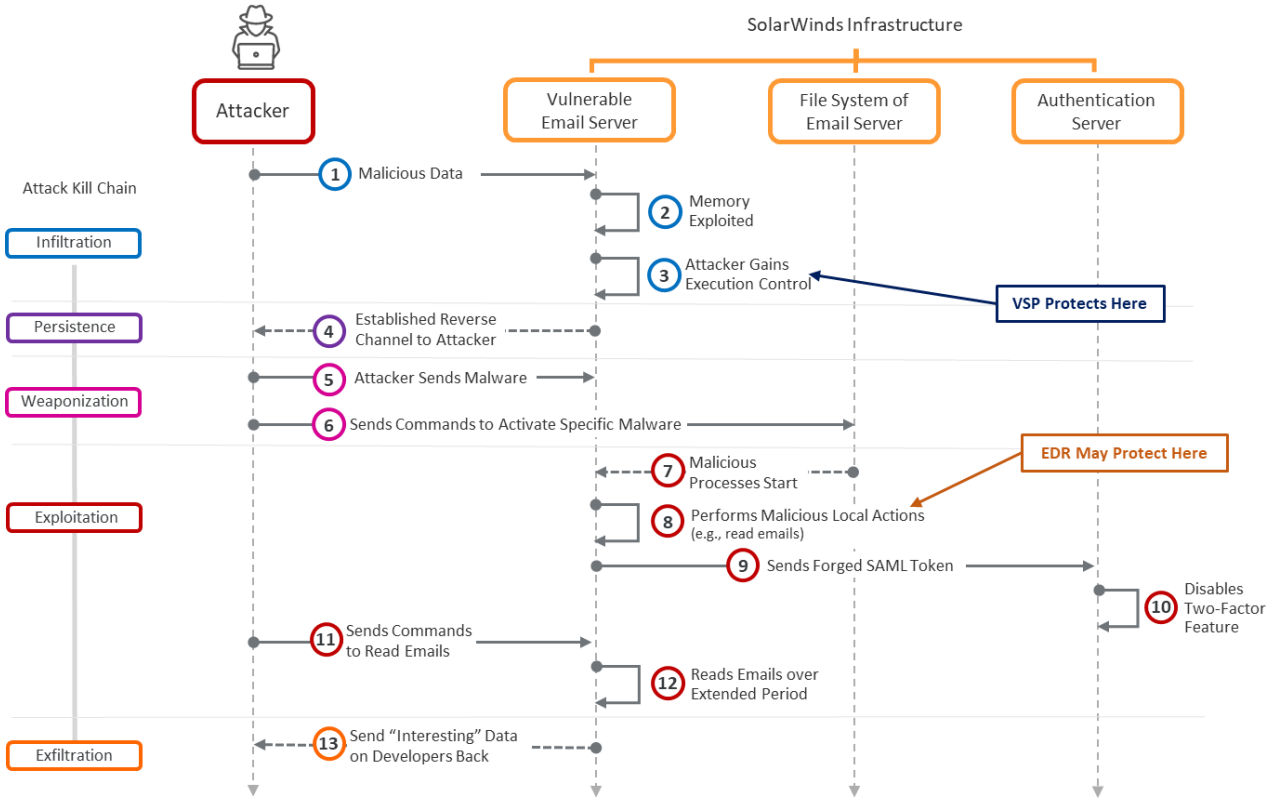

Figure 2: Virsec protection against RCE vulnerabilities

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