LAYER SEVEN SECURITY

SOFTWARE SUPPLY CHAIN ATTACKS

SECURING SOFTWARE SUPPLY CHAINS FOR SAP SYSTEMS

SOFTWARE SUPPLY CHAIN ATTACKS

WHAT ARE SOFTWARE SUPPLY CHAIN ATTACKS?

Software supply chain attacks are advanced cyber attacks that target information systems through third party software. Threat actors compromise systems and data by exploiting software builds or interfaces for trusted software. This enables attackers to introduce malware without detection including backdoors.

solarwinds

WHAT'S THE IMPACT?

30,000	**Microsoft** Up to 30,000 organizations were targeted by software supply chain attacks via flaws in Microsoft's Exchange Server
18,000	**SolarWinds** An estimated 18,000 organizations installed trojanized updates from SolarWinds
$10 BILLION	**WannaCry/ NotPetya** The damages caused by the WannaCry/ NotPetya attacks are estimated at over $10 billion

WHAT HAPPENED AT SOLARWINDS?

The software supply chain attack experienced by SolarWinds is widely regarded as one of the most devastating cyber attacks in history. It impacted as many as 425 of the US Fortune 500, the top ten US telecommunications companies, the top five US accounting firms, all branches of the US Military, the Pentagon, the State Department, the world's largest cybersecurity firm, as well as thousands of organizations worldwide.

The attack targeted the Orion Platform used for SolarWinds products including tools for automated patch management and security & compliance. According to SolarWinds, the initial breach is suspected to have occurred in September 2019. The attackers subsequently modified an Orion plug-in that was distributed as trojanized updates to SolarWinds customers from February 2020. This trojan included a backdoor that provided access to customer networks. The attack remained undetected until December 2020.

SOFTWARE SUPPLY CHAIN ATTACK VECTORS

01

DESIGN

Third party software may include malware embedded by design. The cybersecurity software company ERPScan was sanctioned by the U.S government in 2018 due to alleged ties with Russian intelligence that cast doubts over the integrity of its software.

02

DEVELOPMENT

Software development procedures at third party software vendors may be compromised by attackers to inject malware into software builds that are distributed to customers.

03

DISTRIBUTION

Software builds may be compromised after development during the delivery phase. Codesigning is used to protect the integrity of code. However, codesigning is routinely undermined by threat actors.

04

MAINTENANCE

Software updates and external interfaces required for the delivery of updates may be compromised to introduce malware or hijack remote connections from trusted sources.

COMMON ATTACK TECHNIQUES

Open Source Software

Third party software can include substantial blocks of open source code. This includes platforms and libraries. The use of open source components has increased by 259% over the last 5 years. Applications contain an average of 528 open source components. Open source packages and repositories can include malicious code. They also need to be regularly patched for known security vulnerabilities by software vendors that use the dependencies in their builds. Open source software components contain an average of 158 vulnerabilities per code base. Vulnerabilities in open source software are closely monitored and targeted by attackers since they provide threat actors with many potential exploit victims.

Software Updates

Software vendors typically deliver patches and updates from centralized servers to customers through remote connections. Threat actors can compromise the contents of updates both at source by infiltrating vendor networks or during transmission by intercepting and modifying software distributions. The NotPetya attack was originally spread through malware included in updates for a popular tax accounting program. Vendors often seal software updates with self-signed certificates to authenticate packages. Digital certificates do not protect against malicious updates if the malware is injected at source. Threat actors are capable of hijacking software updates during transmission and bypassing or compromising certificates to disguise malware in payloads as trusted software updates.

SECURING THE SOFTWARE SUPPLY CHAIN FOR SAP SYSTEMS

Minimize Third Party Software in SAP Landscapes
Reduce usage of third party software and rely on SAP platforms for system administration, maintenance and security. Avoid the use of plugins, consoles and sensors that connect to SAP systems, often with privileged access to SAP applications.

Avoid External Connections to SAP Systems
Review and minimize external connections between SAP systems and untrusted networks. Do not rely exclusively on firewall rules or transport layer security to control, authenticate and encrypt remote connections since these mechanisms can be bypassed by threat actors.

Block Third Party Tools Containing Open Source Software
Developers of propriety software routinely leverage blocks of open-source code in their products. This includes vulnerable operating systems such as Ubuntu and potentially malicious python and other libraries. Promote the use usage of closed source software over open source software.

Monitor Third Party Software
Isolate third party software components in separate sub-networks from SAP systems. Harden the components and monitor the actions of agents, plugins and users leveraged by third party tools. Apply vendor patches immediately and implement threat detection and incident response to detect and respond to security breaches in third party software.

NIST RECOMMENDATIONS

The National Institute of Standards and Technology (NIST) recommends eight specific Cyber Supply Chain Risk Management (C-SCRM) practices for identifying, assessing and mitigating risks associated with the use of third party software. This includes extending internal standards for the software development lifecycle to external suppliers. It also includes maintaining component inventories for third party software to identify open source components. External interfaces should be mapped and baselined. Baselining supports the detection of anomalies in the usage of interfaces. Network segmentation is recommended as part of a zero trust architecture. Configuration management is recommended to secure third party software settings and changes.

MANAGING SECURITY WITH SAP SOLUTION MANAGER

NIST CYBER SUPPLY CHAIN RISK MANAGEMENT PRACTICES	SAP SOLUTION MANAGER	THIRD PARTY SOFTWARE
INVENTORY SOFTWARE COMPONENTS The Landscape Management Database (LMDB) in SAP Solution Manager details software components and versions	✓	✗
MINIMIZE EXTERNAL CONNECTIONS SAP Solution Manager does not require any external connections to untrusted networks. Patch updates and notes analysis is performed via a direct connection to SAP Support	✓	✗
AVOID OPEN SOURCE COMPONENTS SAP Solution Manager is a closed-source enterprise platform from SAP. It does not include vulnerable open-source software	✓	✗
MONITOR SECURITY PLATFORMS SAP Solution Manager performs self-monitoring for security incidents, patches and vulnerabilities	✓	✗
MONITOR INTERFACES Interface Monitoring in SAP Solution Managers identifies and monitors the usage of external connections for anomalies	✓	✗
APPLY SECURITY PATCHES System Recommendations in SAP Solution Manager automates the discovery and implementation of SAP security notes	✓	✗

SAP-RECOMMENDED PLATFORM FOR SAP CYBERSECURITY

SAP Solution Manager supports lifecycle management for SAP systems including design, deployment and maintenance. It provides a centralized platform for monitoring systems, managing changes, applying patches and updates,, and other basis functions. SAP Solution Manager also supports security scenarios including vulnerability management, alerting, and incident management. Solution Manager is recommended by SAP for building and sustaining secure system landscapes. Download the SAP whitepaper *Managing Security with SAP Solution Manager* from SAP Support.

LAYER SEVEN SECURITY

Layer Seven Security is a leading provider of cybersecurity solutions and services for SAP systems. The company is recognized as one of the Top 10 SAP Solution Providers of 2018 and Top 25 Cybersecurity Companies of 2020. Layer Seven Security is an SAP Partner and headquartered in Toronto, Canada.

Cybersecurity Extension for SAP

The Cybersecurity Extension for SAP® Solutions automates vulnerability management, threat detection, and incident response to secure SAP platforms against advanced persistent threats including ransomware. The SAP-certified extension protects on-premise, cloud and hybrid SAP systems including S/4HANA, HANA, ABAP and J2EE platforms. It delivers near real-time security intelligence to detect vulnerabilities and indicators of compromise using SAP-recommended applications. The Extension does not require open source software or remote connections to external networks. Furthermore, it uses preexisting agents and users in SAP systems.

SIEM Integrator for SAP

The SIEM Integrator for SAP delivers automated threat detection for SAP systems. The add-on includes over 500 attack detection patterns for SAP and supports fast, seamless integration with SIEM platforms including Splunk, QRadar and ArcSight.

CONTACT US

www.layersevensecurity.com
info@layersevensecurity.com

SAP Partner