Quick Answer: How to Respond to a Supply Chain Attack?

Published 21 December 2020 - ID G00742079 - 5 min read

Peter Firstbrook

Initiatives: Security Operations; Infrastructure Security

Supply chain attacks are a reality, but organizations are often unprepared to respond to a cybersecurity event when it occurs. Security and risk management leaders should have an incident response plan prepared to deal with events where supply chain attacks may impact their organizations.

Additional Perspectives

- Summary Translation: Quick Answer: How to Respond to a Supply Chain Attack? (14 January 2021)

Quick Answer

What is a supply chain attack and how should I respond when it happens?

A supply chain attack is when goods, services or technology supplied by a vendor to a customer have been breached and compromised, which introduces a risk to the customer base. The risk to an organization will vary.

A recent example is the attack against SolarWinds, summarized below:

- The malicious code was distributed as an in-line modification to an otherwise legitimate software update to the SolarWinds Orion platform servers. The updated code with the malicious implant was signed using valid SolarWinds digital certificates. Following a reboot of the server, the malware (which is running with administrative privileges) collects details of running security processes and services on the host. It then disables the processes and services through modifications to the Windows registry.

- The malware starts communicating with attacker-controlled infrastructure (i.e., beaconing) in order to identify the compromised network to the attacker. This attacker-controlled infrastructure can enable a second round of command and control (C2) communications.

- The malware uses various evasion techniques to avoid detection. It leverages existing SolarWinds Orion configuration files and attempts to blend with the compromised network, as the C2 communications use the same protocol as SolarWinds (Orion Improvement Program protocol). The malware modules have names that are similar to SolarWinds modules. “In country” relays are utilized for C2 in order to achieve the appearance of legitimate traffic.
In subsequent stages of the attack, the attackers exploit administrative permissions to gain access to the organization's global administrator account and SAML certificate, enabling subsequent authentications to other services, which can impersonate any existing SAML account and the creation of new privileged accounts. Microsoft has released customer guidance on recent nation-state cyber attacks.

More Detail

For more detail related to the SolarWinds event in December 2020, please refer to:

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor, FireEye.

The affected versions of SolarWinds Orion products that are currently being exploited by malicious actors are 2019.4 through 2020.2.1 HF1. An attacker is able to gain access to network traffic management systems. As described in United States Department of Homeland Security material, current guidance indicates that disconnecting affected devices and updating them is the only known mitigation measure currently available.

Orion servers and network and endpoint logs should be inspected for known indicators of compromise (IOCs). Any detection of IOCs should result in a full-scale incident response investigation by qualified professionals.

Public documentation of SolarWinds breach details from external sources offers several of the following details. However, these details are subject to change as more is learned. We provide general guidance on the SolarWinds breach, but this is not a substitute for a full incident response investigation.

The system and network compromises are not self-propagating, and each of the attacks requires meticulous planning and manual interaction. Types of attack include:

- Attacks on the supplier's technology (software, hardware), which implant backdoors via that technology to allow an attacker to compromise a customer once the software or hardware has been deployed.
- Attacks on the supplier's IT network, which involve remote access or network connectivity between the supplier's network and the customer's network.
- Attacks on the supplier's IT environment, where it is hosting or managing IT infrastructure on behalf of a customer, which is then attacked and compromised.
- Attacks on supplier's email system (vendor email compromise), which is then used to facilitate attacks on customers.

How should you respond to a supply chain attack?
The assumption is that attacks of this nature can occur at any time from any product or vendor. Security and risk management (SRM) leaders must have tools to detect the lateral movement from the initial compromised service, and an incident response plan for attacks against the supply chain with an agreed workflow to manage a coordinated reaction.

The plan should include several steps.

First, determine if the organization or a critical third-party is affected. If the team determines that the organization is affected, use known indicators of compromise and user activity logs to track lateral movements. Reach out to your security vendors to quickly learn about updates and suggested analysis workflows.

If necessary, engage qualified incident response organizations. Consider the value of a retainer incident response service that can be engaged at the first sign of compromise without the burden of rushed contractual negotiations.

Determine the balance between rebuilding or cleaning for compromised hosts and credentials. Engage in more active monitoring to spot potentially related anomalies.

Have a supply chain risk management function if feasible; at the least, have a documented list of critical suppliers and vendors in the event a breach is reported. (See Combat Digital Security Threats to the Supply Chain.)

Endpoint detection and response, network detection and response, and identity management tools are critical for detecting lateral movement and anomalies in the credential management system.

Gartner recommends managed detection and response (MDR) for any organization that does not have enough qualified security analysts to do detection on a comprehensive basis. Also worth deploying are tools that incorporate user behavioral analytics to examine standard access behavior of users and servers. If such a tool is deployed, it will help reduce the spread of malware by limiting it to the systems the infected device can access.

When acquiring any new software, request from the vendor information about the last time a complete independent code review was performed and the schedule for regular audits of code. It is also important to request a list of servers and ports that any software would need to communicate with.

Any network security with threat intelligence or signatures could detect the C2 communication once the servers are known as bad. This includes intrusion detection and prevention systems (IDPS), secure web gateways (SWGs), firewall, and network detection and response (NDR) that monitor north-south traffic if deployed in front of the SolarWinds servers. DNS security could also detect the identified domains. These NDR systems might detect abnormal activity, including “unusual connection to an unknown server,” “abnormal volume of data to external server” and other network anomalies.
However, for C2 and malware detections, there is at least one important consideration: SolarWinds servers are likely to be in a “management” segment, and might not go through the same network security controls as the user segments (e.g., no traffic decryption, or a different SWG or IDPS policy). If possible, protect software in a management segment stringently, allowing least possible contact between the management software and the systems it must interact with.

**Recommended by the Authors**

- Market Guide for Digital Forensics and Incident Response Services
- Market Guide for Managed Detection and Response
- Market Guide for Endpoint Detection and Response
- Market Guide for Network Detection and Response
- Innovation Insight for Extended Detection and Response
- Magic Quadrant for Security Information and Event Management
- Ignition Guide to Developing a Security Incident Response Plan
- Build Your Security Incident Crisis Communications Plan
- How to Implement a Computer Security Incident Response Program