Network Behavior Analysis of critical software for detecting software supply chain attacks

Author: Edward Wu, Extrahop Networks

Applies to area 3: Guidelines outlining security measures that shall be applied to the federal government's use of critical software

One of the innate signs of software supply chain attacks is the deviation from normal behaviors after the software system has been compromised. For example, in SUNBURST attacks, compromised systems sent unusual DNS requests for malicious domains such as avsvmcloud[.]com and made unusual connections (compared to a benign SolarWinds installation) to internal systems across the network (a characteristic of lateral movement attacks). Based on these observations and the practical deployment advantages, we propose that NIST recommends the prioritization and implementation of Network Behavior Analysis as a security measure to detect and stop future novel software supply chain attacks.

How the Network Behavior Analysis works

Network Behavior Analysis consists of two components.

The first component involves out-of-band monitoring the network traffic of critical software systems with network sensors. By mirroring network traffic through a SPAN port or packetbroker, network sensors passively ingest network packets and generate metadata (aggregated metrics or logs) that summarizes the traffic. Out-of-band monitoring enables security teams to obtain a comprehensive picture of the attack surface for these systems, covering both north-south (inbound and outbound traffic) and east-west (lateral movement traffic within the private network) communications of critical software systems.

The second component involves an analytical module for reviewing observed network traffic of critical software systems, identifying expected behavior, and detecting deviations from expected behavior. Security teams could manually write policies for the expected traffic that is reviewed by this module and create alerts for policy violations. Security teams could also leverage machine learning (ML) technology to dynamically learn about the expected traffic for each critical software installation and surface alerts for deviations from expected behaviors. After an alert is surfaced, the security team investigates network traffic (metrics, logs, or packets) and other security data sources (threat intelligence) to determine the cause. Security teams also have the option of integrating this module within their switch and router infrastructure to immediately cut off the suspicious network traffic.

A devastating aspect of a supply chain attack is the hijacking of trusted services and privileges, which enable attackers to compromise internal targets and persist on the network. SUNBURST attackers gained access to SolarWinds installations, and blocked anti-virus and other endpoint security tools from detecting their presence. But these adversaries can't hide their attack behaviors, which are detectable with Network Behavior Analysis. Attackers must connect to external servers to maintain control of their compromised devices, and they must probe the internal networks to find new targets. Because Network Behavior

Analysis identifies the expected network behavior of SolarWinds installations, it detects unusual DNS requests to malicious command-and-control server domains. Network Behavior Analysis also identifies unusual connections (over remote access protocols, for example) to internal systems that indicate an attacker is pivoting to new internal targets.

Comparison to traditional network defenses

Network segmentation is an extremely useful mechanism to mitigate and detect attacks, but it is rarely adopted in large, complex network environments. Network segmentation requires extensive planning and continuous maintenance of routing policies and ACLs, ensuring that segments don't affect business-critical traffic. For these reasons, network segmentation might only be deployed for specific scenarios, such as guest access and data center communication. Critical software systems might be installed in unsegmented portions of the network to allow for broad, undisrupted access to these systems. But broad access means that an attacker can easily move laterally from a compromised system to other parts of the network.

The Network Behavior Analysis leverages out-of-band monitoring for networks that lack segmentation. Instead of segmenting the network to prevent A from talking to B, it uses out-of-band monitoring to identify normal network traffic and simply surface an alert when A unexpectedly talks to B. While segmentation builds walls that an attacker would need to navigate around, Network Behavior Analysis installs invisible tripwires that immediately alert security teams as soon as the attacker makes their move.

Application-layer mutual authentication is a well-known approach to implement Zero Trust networking. This approach is more granular and flexible than network segmentation. Every application running on each network device is expected to be mutually authenticated on the application layer, regardless of network access. It’s akin to putting a keycard scanner on every drawer in the whole building and leaving every single door unlocked in the physical world. While this approach provides very granular control and good security practices, it is hard to implement. Users need to ensure they are authenticated and application owners must make modifications to ensure compliance. In comparison, Network Behavior Analysis does not require any consent or coordination with the internal owners of critical software systems, and legacy critical software installations are secured without any modifications.

In conclusion, Network Behavior Analysis is a non-intrusive, practical, roburst, and complementary measure to traditional network security defense approaches, such as network segmentation and application-layer mutual authentication. Network Behavior Analysis is effective at detecting and stopping software supply chain attacks because it is able to secure any critical software installations, regardless of methods of actual supply chain attacks. It is also a out-of-band system, reducing the burden of deployment in complex networks or environments with legacy critical software systems. Organizations of any size or shape can implement Network Behavior Analysis to enhance security for critical software systems and rapidly increase its Zero Trust maturity. As a result, we propose that NIST recommends the prioritization and implementation of Network Behavior Analysis as a security measure to detect and stop future novel software supply chain attacks.