Global Intrusion Campaign Leverages Software Supply Chain Compromise

fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html

FireEye Stories Blog

December 13, 2020 | by Kevin Mandia
FireEye

In our announcement on Dec. 8, we stated we would provide updates as we discovered additional information, in order to ensure that the broader community is aware of the evolving threats we all face. As part of that commitment, we want to provide you with the following update on our investigation.

We have identified a global campaign that introduces a compromise into the networks of public and private organizations through the software supply chain. This compromise is delivered through updates to a widely-used IT infrastructure management software—the Orion network monitoring product from SolarWinds. The campaign demonstrates top-tier operational tradecraft and resourcing consistent with state-sponsored threat actors.

Based on our analysis, the attacks that we believe have been conducted as part of this campaign share certain common elements:

- **Use of malicious SolarWinds update**: Inserting malicious code into legitimate software updates for the Orion software that allow an attacker remote access into the victim's environment
- **Light malware footprint**: Using limited malware to accomplish the mission while avoiding detection
- **Prioritization of stealth**: Going to significant lengths to observe and blend into normal network activity
- **High OPSEC**: Patiently conducting reconnaissance, consistently covering their tracks, and using difficult-to-attribute tools

Based on our analysis, we have now identified multiple organizations where we see indications of compromise dating back to the Spring of 2020, and we are in the process of notifying those organizations. Our analysis indicates that these compromises are not self-propagating; each of the attacks require meticulous planning and manual interaction. Our ongoing investigation uncovered this campaign, and we are sharing this information consistent with our standard practice.

We have been in close coordination with SolarWinds, the Federal Bureau of Investigation, and other key partners. We believe it is critical to notify all our customers and the security community about this threat so organizations can take appropriate steps. As this activity is the subject of an ongoing FBI investigation, there are also limits to the information we are able to share at this time.

We have already updated our products to detect the known altered SolarWinds binaries. We are also scanning for any traces of activity by this actor and reaching out to both customers and non-customers if we see potential indicators.

For more information please see:

- Technical details regarding the actor's tactics, techniques and procedures
- FireEye's GitHub for SUNBURST countermeasures
- SolarWinds Security Advisory

FireEye's mission is to make our customers and the broader community safer. We are methodically uncovering and exposing this campaign piece by piece and working to prevent future attacks. It will require coordinated action by public and private organizations to fully expose and mitigate this threat, and we intend to continue our efforts.

Forward Looking Statements

Certain statements contained in this blog post constitute "forward-looking statements" within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended. These forward-looking statements are based on our current beliefs, understanding and expectations and may relate to, among other things, statements regarding our current beliefs and understanding regarding the

impact and scale of the disclosed event and our understanding of what occurred. Forward-looking statements are based on currently available information and our current beliefs, expectations and understanding, which may change as the investigation proceeds and more is learned, including what was targeted and accessed by the attacker. These statements are subject to future events, risks and uncertainties – many of which are beyond our control or are currently unknown to FireEye. These risks and uncertainties include but are not limited to our ongoing investigation, including the potential discovery of new information related to the incident.

Forward-looking statements speak only as of the date they are made, and while we intend to provide additional information regarding the attack, FireEye does not undertake to update these statements other than as required by law and specifically disclaims any duty to do so.

Previous Post
Next Post