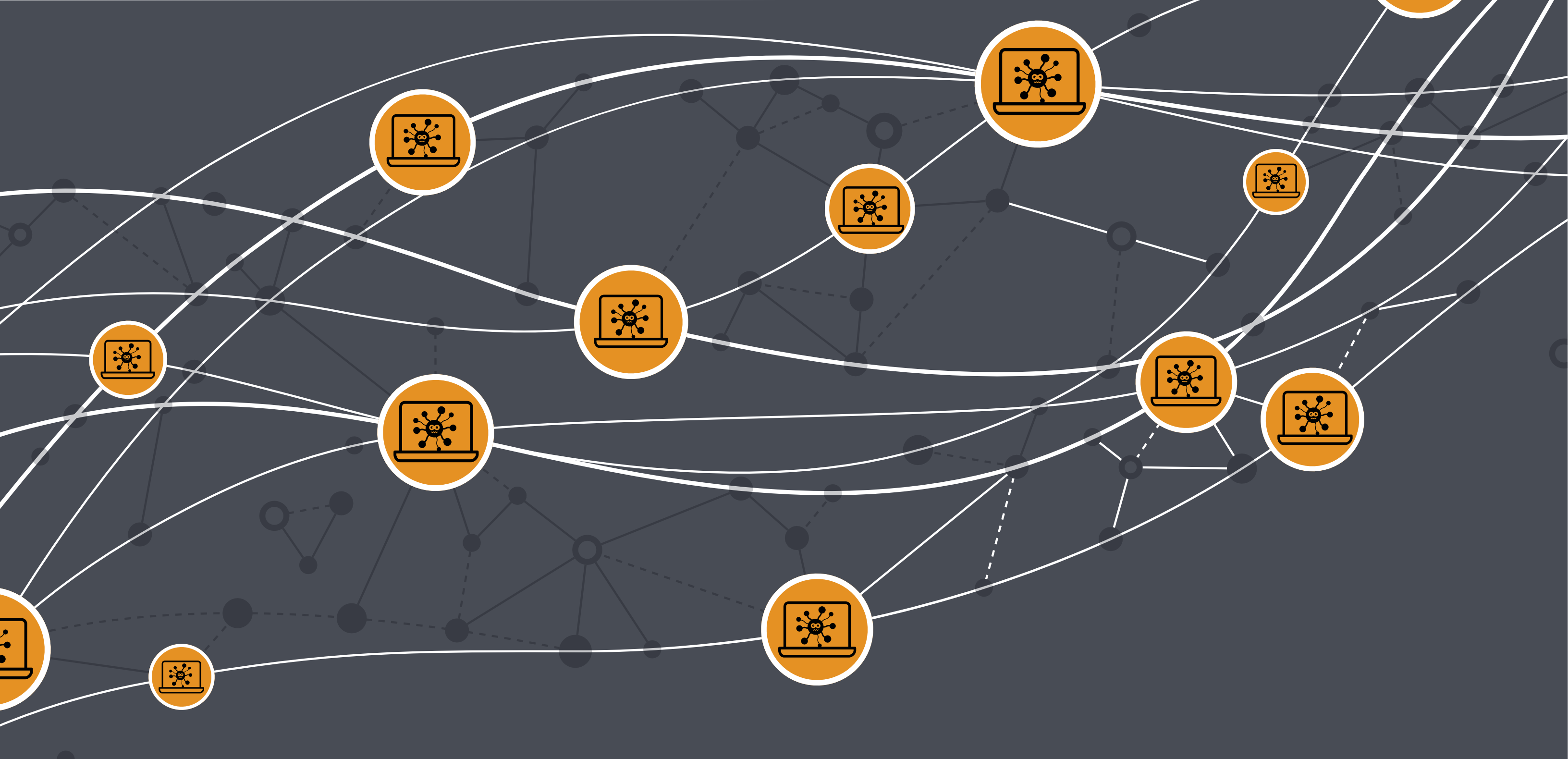

Sunburst: An Attack Timeline

Tracking the events of a supply chain hack

The SolarWinds attack rocked the cybersecurity community with its subtlety, skill and reach. While it wasn't the first, it may have been the most consequential supply chain cyberattack to date. In terms of targets, the audacity of the attack meant that many government agencies were compromised and sophisticated cybersecurity tools were stolen.

Understanding the motives, methods and movements that led to the breach is critical to preventing the next one and limiting the success of similar supply chain attacks could be critical to keeping more businesses from becoming victims.

Here's what the Webroot® Platform saw pertaining to the attack and when.

File Analysis | **URL/IP Analysis**

2019

November 5 & November 7
Compromised SolarWinds files seen on Webroot SecureAnywhere® endpoints

Evidence of attackers "testing" to see if their activity would be noticed is spotted

2020

January 9 – March 5
Seven IPs later identified as part of Sunburst infrastructure classified as spam or high risk

Sunburst indicators of compromise (IOC) first seen

April 7 – December 12
Compromised SolarWinds files and URLs seen among Webroot BrightCloud® and Webroot SecureAnywhere® traffic

June 4

Two files containing actual backdoor compromise seen

July 24
One Sunburst IP classified as Botnet, Phishing, and Proxy

A closer look at the attack discovery.

December 13
The Cybersecurity & Infrastructure Security Agency (CISA) releases Emergency Directive 21-01

UTC 22:33:55
FireEye releases indicators of compromise (IOCs) associated with Sunburst

UTC 03:12:23 – 11:26:21
10 URL IOCs classified as Malwares

UTC 07:51:00
One URL containing compromised SolarWinds downloads classified as Malware

UTC 20:55:04 – 21:25:03
IOCs blacklisted as Windows Exploits

December 14
Entry point rule created to identify new variants

December 14
Microsoft sinkholes key command-and-control server and implements kill-switch

December 14 – Present
Continue to investigate and track new IOCs related to the Sunburst campaign

December 18
Updating category for sink holed C2 server domain to benign to support kill-switch functionality

While every cyberattack is unique, indicators of compromise like foreign files, IPs and URLs are hallmarks of nearly all of them. Having real-time threat intelligence informed by millions of real-world devices, when properly configured, can help stop breaches before they spread.

If you're a technology or IT security vendor in need of threat intelligence to protect your customers, contact sales@brightcloud.com.

If you're an MSP looking to learn more about how real-time threat intelligence is included in Webroot products, you can contact us here.

WEBROOT®
an opentext™ company