- Data Bandwidth
- Internet
- Dark Fiber
- Construction Services

FirstLight®

SolarWinds Hack Explained

- Unified Communications
- Data Center
- Cloud Computing
- Managed Services
- Hardware

Part I

Agenda

- What is SolarWinds - General overview and connectivity
- So, what is this ‘SolarWinds hack’?
- What is a "back door"
- How did so many US government agencies and companies get attacked?
- How did hackers sneak malware into a software update?

What is SolarWinds?

solarwinds

"SolarWinds is a leading provider of powerful and affordable IT infrastructure management software. Our products give organizations worldwide, regardless of type, size, or IT infrastructure complexity, the power to monitor and manage the performance of their IT environments, whether on-premise, in the cloud, or in hybrid models."

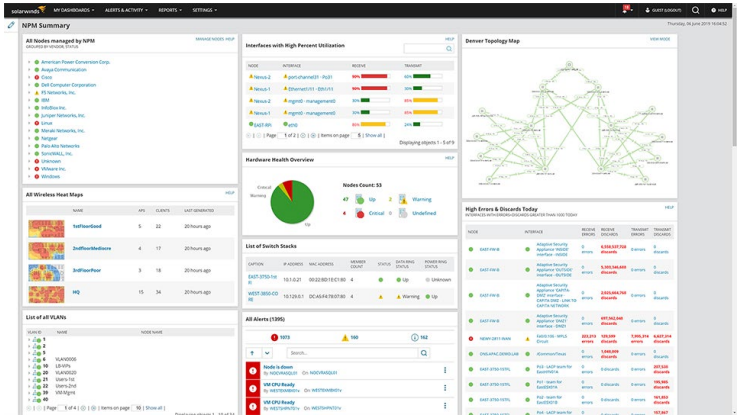
NYSE: SWI

$17.14

-0.10 (-0.55%)

Pricing delayed by 20 minutes

Last Updated 03/16/2021 11:04 am



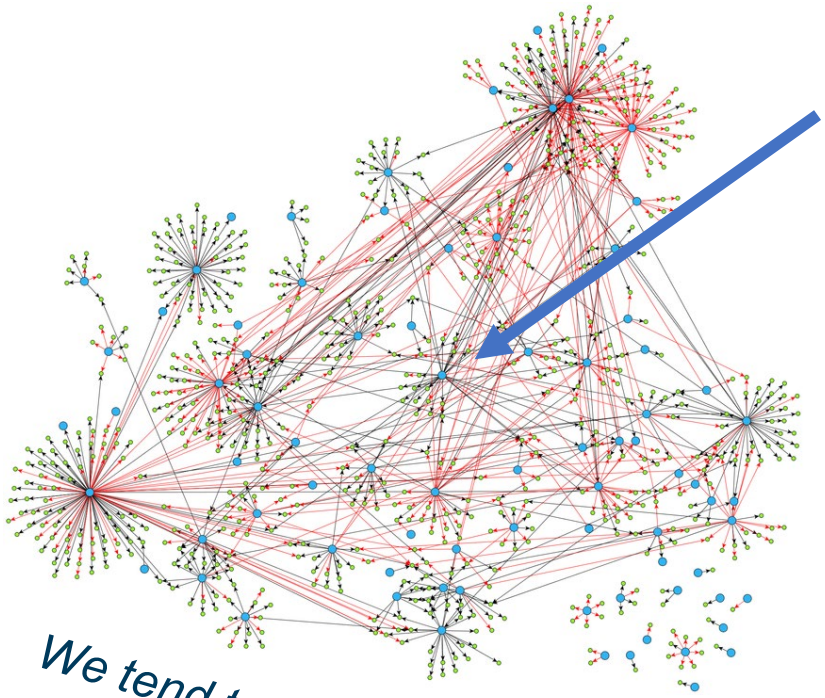
SolarWinds' products serve more than 275,000 customers worldwide

How Big?

SolarWinds stated that its customers included:

- **425 of the US Fortune 500**
- **Top ten US telecommunications companies**
- **Top five US accounting firms**
- **All branches of the US Military**
- **Pentagon**
- **State Department**
- **Hundreds of universities and colleges worldwide..”**

Let's Monitor It All

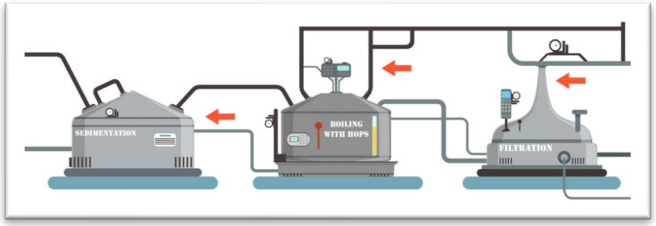


We tend to think and protect ourselves from OUTSIDE → IN.

solarwinds

- We want to monitor it all!
- Even the most important devices MUST get monitored!
- All types of devices from networking to servers, applications, security, cameras, UPS, power and more!
- Monitoring software sits at the heart of the hub spoke.

Hack Overview

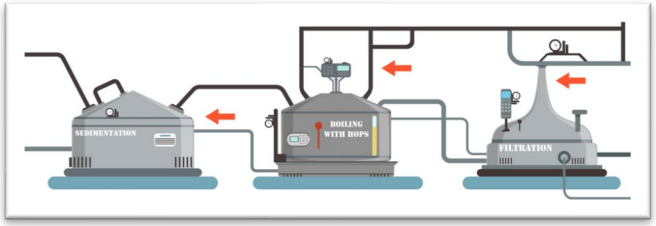


WATER TREATMENT PLANT

Everyday we drink water from a “trusted” source.

If we go to “source” and test, things will look good!

Supply Chain

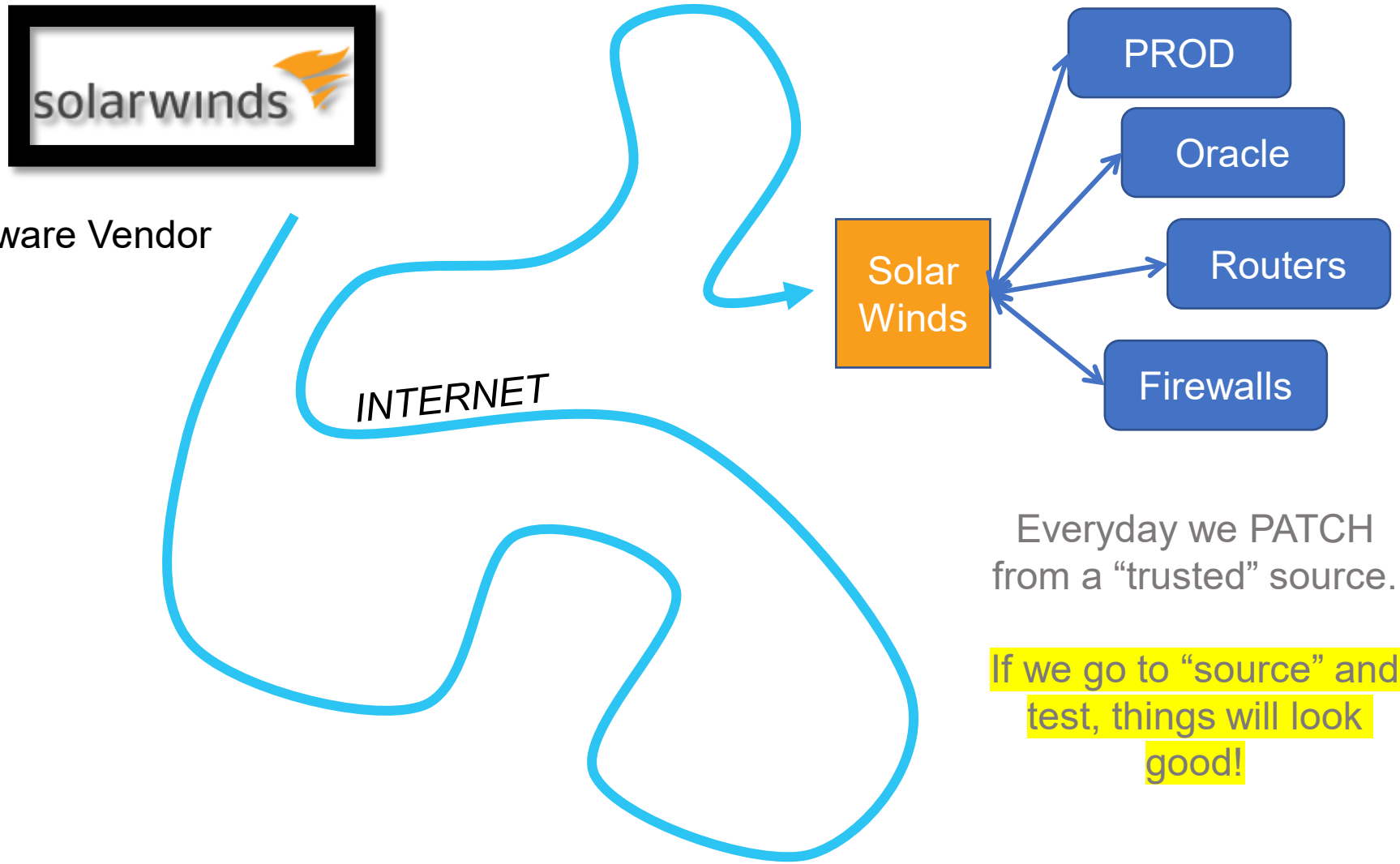


WATER TREATMENT PLANT

Everyday we drink water from a “trusted” source.

If we go to “source” and test, things will look good!

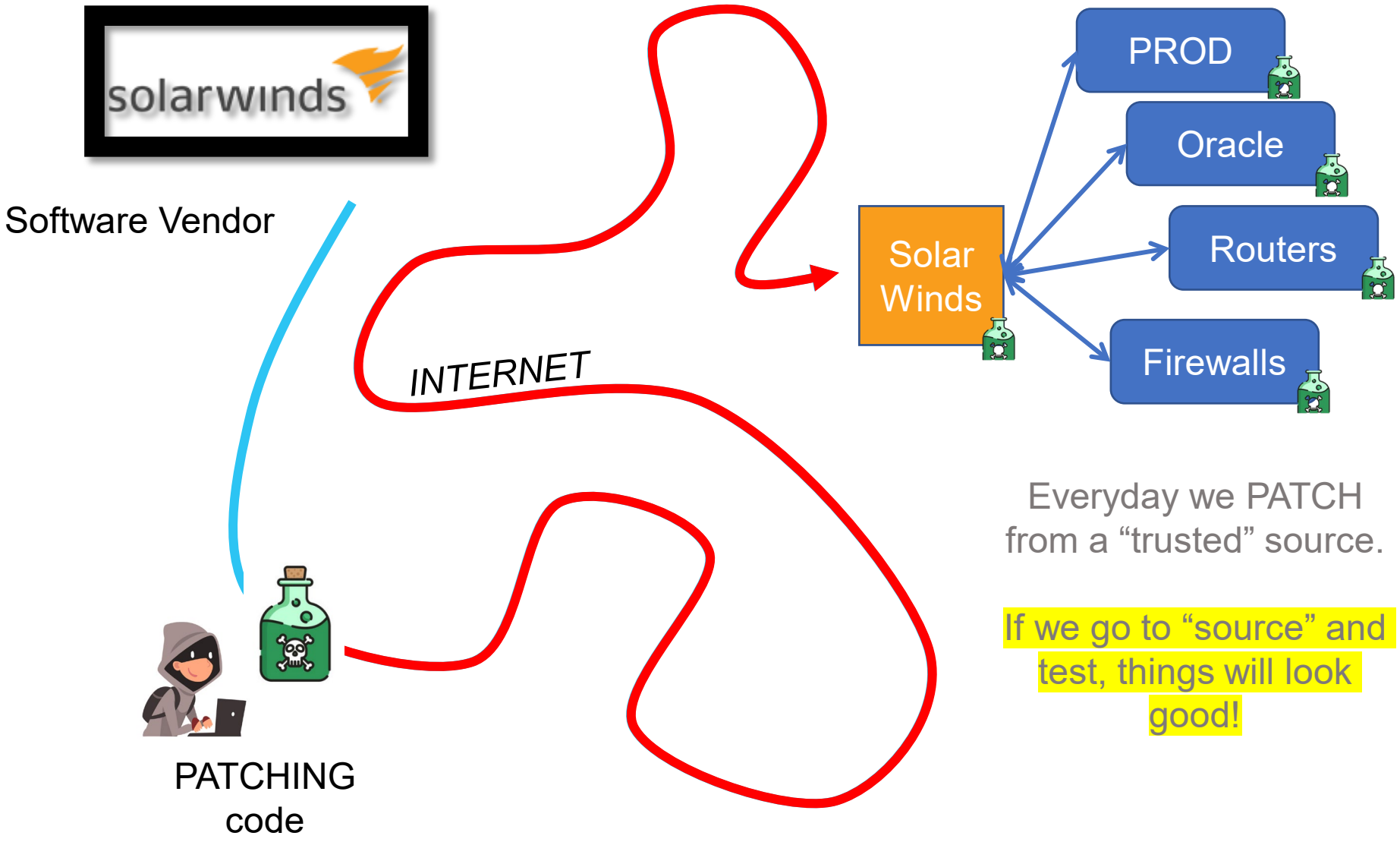
SolarWinds



Everyday we PATCH from a “trusted” source.

If we go to “source” and test, things will look good!

SolarWinds



Everyday we PATCH from a “trusted” source.

If we go to “source” and test, things will look good!

Technical Explanation

solarwinds

"The attackers managed to modify an Orion platform plug-in called **SolarWinds.Orion.Core.BusinessLayer.dll** that is distributed as part of Orion platform updates. The trojanized component is **digitally signed** and contains a backdoor that communicates with third-party servers controlled by the attackers.

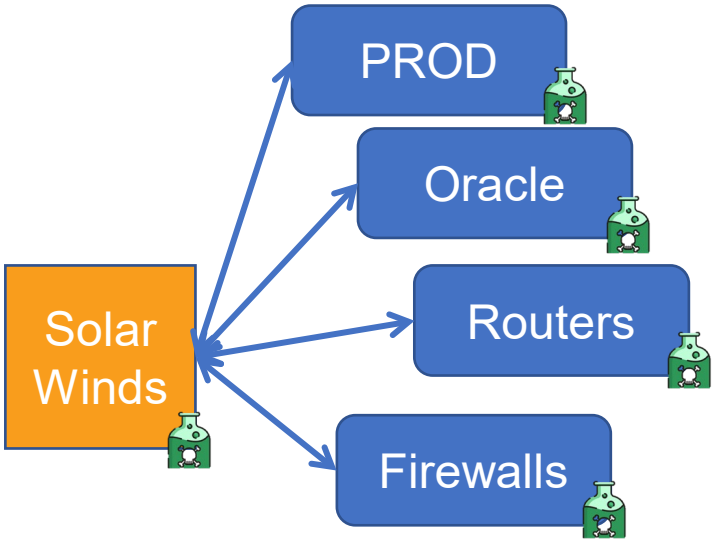
FireEye tracks this component as SUNBURST and has released open-source detection rules for it on GitHub."

SolarWinds

After an initial dormant period of up to two weeks, it retrieves and executes commands with the ability to transfer files, execute files, profile the system, reboot the machine, and disable system services

It's activity blends in with legitimate SolarWinds activity.

Remote Access

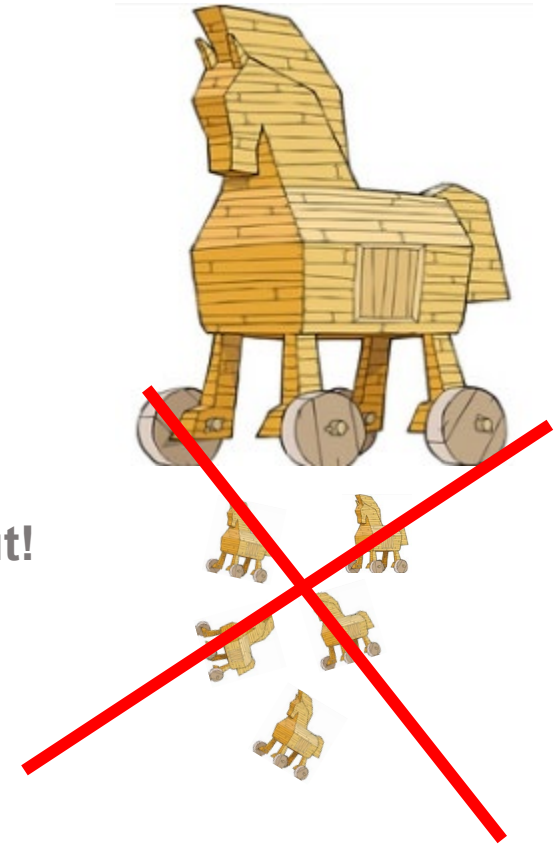


INTERNET

Trojan Horse

Trojan Horses aren't bad!

They're just wooden structures



Baby Horses DON'T Pop Out!

Trojan Horse

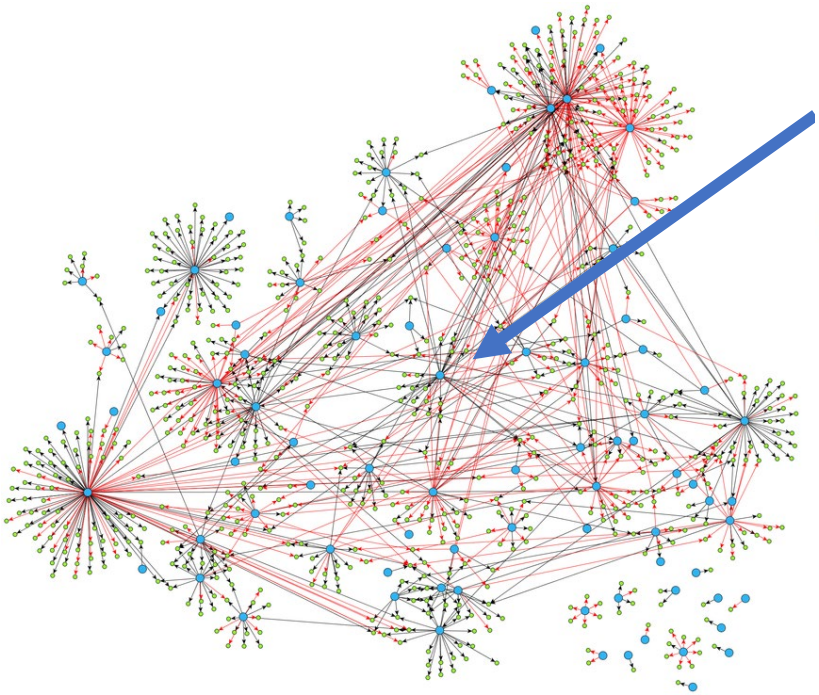
Broken Basement Windows aren't bad!

They're just holes!

First you must find the broken window.

Even after you fix it, who's inside?

Footprint?



X Millions or just 1, both are scary!

- Unlimited number of “Ninjas” that come out of the trojan horse.
- Sitting on a machine that *we* pushed to get access to everything.
- Ability to leave no traces, poke around quietly, act as other programs and report back “home”
- Allows remote commands + control
- What can we trust since this thing can mimic real/trusted objects?

She's Dead Jim!

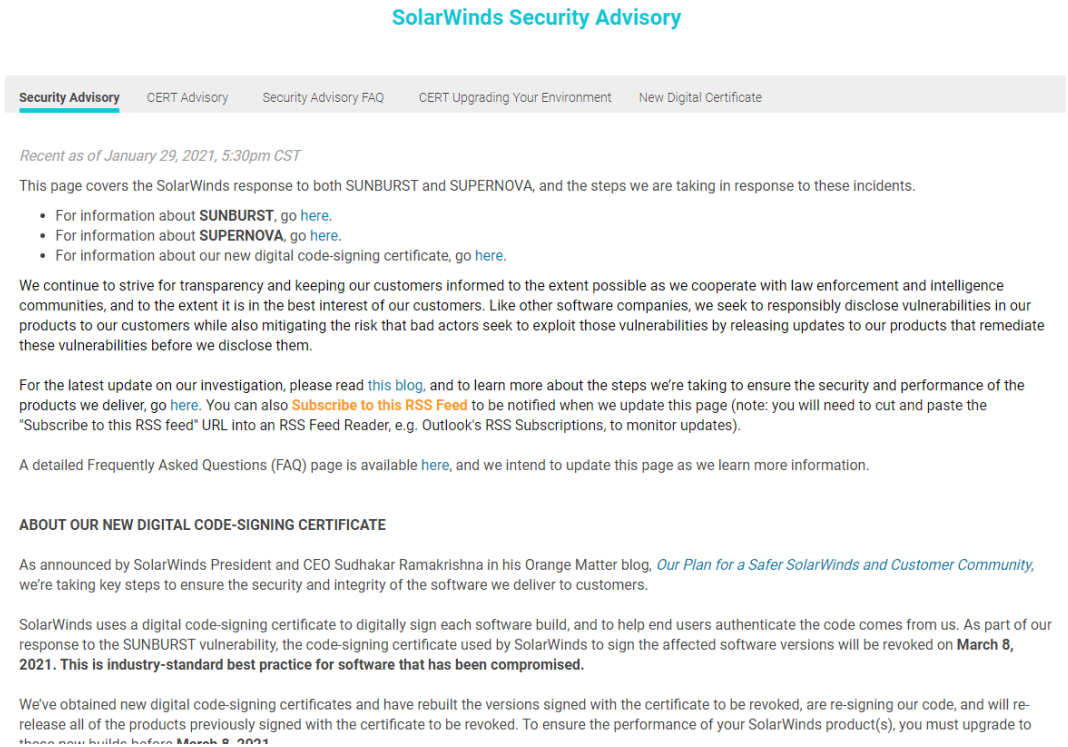
- You've fixed the hole in the basement window but how long has it been there?
- Has anything(s) come through it?
- Have I brought that "thing" with me to other houses, partners, banks, schools, etc?
- Can I trust anything in the house anymore (since this "thing" can mimic real/trusted objects?)

"When I run my virus infected virus scanner, it says I'm good!"

Get Patching!

- For the latest information, be sure to visit SolarWinds security page:

https://www.solarwinds.com/sa-overview/securityadvisory



SolarWinds Security Advisory

Security Advisory | CERT Advisory | Security Advisory FAQ | CERT Upgrading Your Environment | New Digital Certificate

Recent as of January 29, 2021, 5:30pm CST

This page covers the SolarWinds response to both SUNBURST and SUPERNOVA, and the steps we are taking in response to these incidents.

- For information about **SUNBURST**, go here.
- For information about **SUPERNOVA**, go here.
- For information about our new digital code-signing certificate, go here.

We continue to strive for transparency and keeping our customers informed to the extent possible as we cooperate with law enforcement and intelligence communities, and to the extent it is in the best interest of our customers. Like other software companies, we seek to responsibly disclose vulnerabilities in our products to our customers while also mitigating the risk that bad actors seek to exploit those vulnerabilities by releasing updates to our products that remediate these vulnerabilities before we disclose them.

For the latest update on our investigation, please read this blog, and to learn more about the steps we're taking to ensure the security and performance of the products we deliver, go here. You can also **Subscribe to this RSS Feed** to be notified when we update this page (note: you will need to cut and paste the "Subscribe to this RSS feed" URL into an RSS Feed Reader, e.g. Outlook's RSS Subscriptions, to monitor updates).

A detailed Frequently Asked Questions (FAQ) page is available here, and we intend to update this page as we learn more information.

ABOUT OUR NEW DIGITAL CODE-SIGNING CERTIFICATE

As announced by SolarWinds President and CEO Sudhakar Ramakrishna in his Orange Matter blog, *Our Plan for a Safer SolarWinds and Customer Community,* we're taking key steps to ensure the security and integrity of the software we deliver to customers.

SolarWinds uses a digital code-signing certificate to digitally sign each software build, and to help end users authenticate the code comes from us. As part of our response to the SUNBURST vulnerability, the code-signing certificate used by SolarWinds to sign the affected software versions will be revoked on **March 8, 2021. This is industry-standard best practice for software that has been compromised.**

We've obtained new digital code-signing certificates and have rebuilt the versions signed with the certificate to be revoked, are re-signing our code, and will re-release all of the products previously signed with the certificate to be revoked. To ensure the performance of your SolarWinds product(s), you must upgrade to