Step one: Infiltrate Solarwinds

Who is APT29?

Origin: Russia
Purpose: Hacking, spying, stealing

Classified by the US Federal Government as "Advanced Persistent Threat" ATP29, is a Russian hacker group believed to be associated with one or more intelligence agencies of Russia. They hunt for confidential information in governmental, political, and think tank organizations.

APT29

Who is Solarwinds?

Origin: USA
Purpose: Cyber defence & management

SolarWinds is a software company based in the United States that aids businesses maintain their networks, systems, and information technology infrastructure by offering different solution products.

It had about 300,000 customers as of December 2020, including nearly all Fortune 500 companies and several federal agencies.

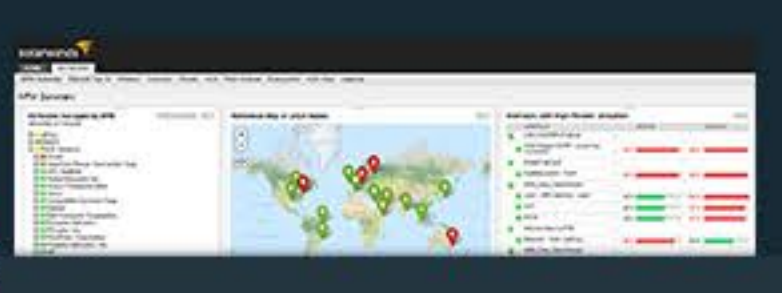
solarwinds

Method of entry: unknown

The biggest mystery is how the hackers managed to breach Solarwinds network in the first place.

- **Phishing attacks?**
  Emails containing infected attachments could have been downloaded by a Solarwinds employee.
- **Code backdoor?**
  Solarwinds have been using developers from outside the US, closer to the Russian sphere of influence.
- **Weak password?**
  Security researchers have discovered weak and openly available passwords for Solarwinds products.

Step two: Infect the Orion Network



Orion targeted

Orion is a suite of tools that help organizations to monitor and manage their computer networks and servers.

INFILTRATED

Update Server

APT29 issues a malicious update from Solarwinds trusted server to all of its Orion customers.

solarwinds

Einstein fails

USA spent billions of dollars on Einstein, an intrusion detection system, only to have it fail to detect the biggest intrusions to date.

FAILED

Trojan spreads

The update was installed by over **18.000** Orion customers, creating a backdoor for the APT29 hackers.

Dep. of Homeland Security
State Departement
Department of Energy
Department of the Treasury
Department of Energy
Department of Commerce
National Nuclear Security Adm.
National Institute of Health
Dep. of State Hospitals
Kent State University
Iowa State University
Pima County
Microsoft
Cisco
Intel
Deloitte
Belkin
Nvidia
WMware
FireEye

Step three: Collect Information

The ***biggest*** *hack America has ever seen.*

Backdoor went undetected for 9 months

The breach began as early as March 2010 and went unnoticed for 9 months. During that time the APT29 group had access to information flowing through the White House, The Pentagon, The treasury, and **425 of Fortunes 500 companies.**

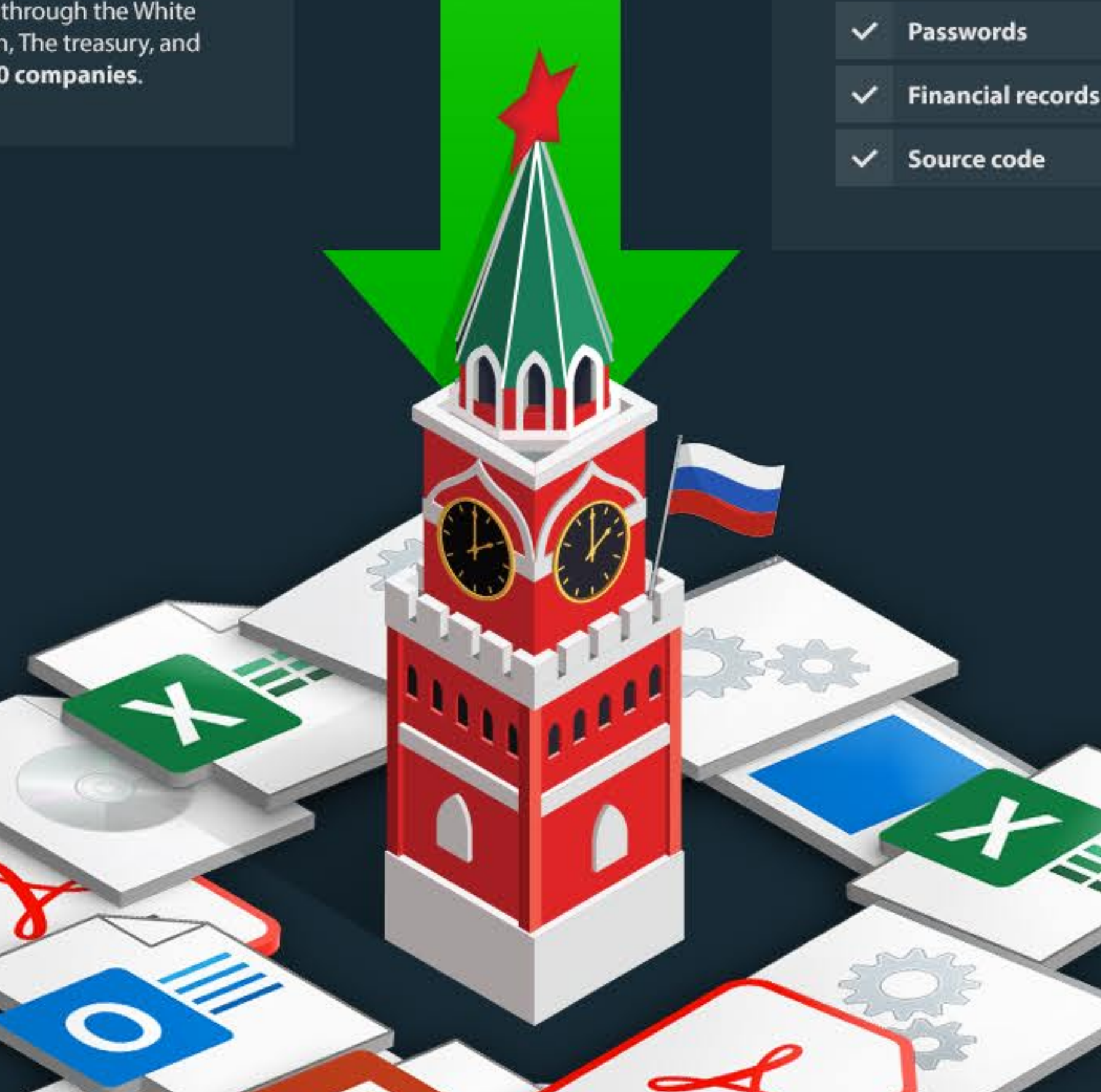
Backdoor installed

With a backdoor to most of SolarWinds high profile customers, APT29 can start collecting information about their targets.

Spying on targets

The data within these networks can be presumed now to be in the hands of Russian intelligence agents.

- ✓ User ID's
- ✓ Passwords
- ✓ Financial records
- ✓ Source code



Step four: U.S. Damage Control

Cleaning up

The job of completely removing the hacker's presence over the breached networks is, to say the least, a **mammoth task**. Since the attack went undetected for months the hackers could have planted backdoors and other malicious code anywhere, making the task of removal almost impossible.

> *"It's like knowing a burglar has been in your house, but you don't really know what they took, so you have to go into every room, and inventory everything of value everywhere before you have confidence of knowing what the impact was,"*
>
> - Steve Grobman, the chief technology officer at McAfee, a cybersecurity company.

> *"It's certainly going to be the worst cyberattack in United States history thus far, and I don't believe people understand its magnitude, It's primarily so troubling because of its alarming scope—**the scale of this is breathtaking.**"*
>
> -Tom Bossert, former Homeland Security adviser.

Even the task of **cleaning up** after the intrusion might be exploited by the hackers. They will attempt to understand exactly how to U.S feral agencies and American companies respond to a hack, using that information to attack with more sophistication in the future.

Cost

While experts debate the cost of fixing and securing all systems after the Solarwinds hack, one thing is clear: it's not going to be cheap. As the scale of the attack still isn't fully known, and experts keep finding out more, most figures will have to be revised upwards.

While large companies might have enough resources to completely rebuild their computer systems, smaller ones do not and might be continuously exploited going forwards.

> *"The reality is everybody is spending resources right now, and the global price tag is likely to be in the billions. The true cost could be **hundreds of billions of dollars.**"*
>
> -Jake Williams, former NSA hacker.