Twitter Thread by Dannielle (Dossy) Blumenthal PhD

Dannielle (Dossy) Blumenthal PhD
@DrDannielle

SolarWinds follow up. Very good tweet explaining what happened.

> Hackers reportedly slipped malware into prior SolarWinds software updates, which gave them access to a "God-mode" for infected networks, including the Treasury and Commerce departments.
>
> The Pentagon is also a SolarWinds customer.https://t.co/Srcoztssol https://t.co/OgMhAjJqPx
>
> — Wes Wilson (@weswilson4) December 14, 2020

Basically what this means is that SolarWinds itself was exploited. Someone posted an infected update as legitimate (digitally signed), leading customers to download a bad update.

“Multiple trojanized updates were digitally signed from March - May 2020 and posted to the SolarWinds updates website” https://t.co/8e3bMFWXYu

FireEye then explains that infected organizations were approached and exploited. This is a separate Step 2.

At this point, information is already going to “malicious domains” without extra intervention, after the malware does nothing for “up to two weeks”

But the cyber thieves take the opportunity to move around (“laterally”) inside the infected organization.

Bad actor = UNC42.
Trojan software = SUNBURST.

Basically the intruder tiptoes around the infected network grabbing more stuff.

As Chris Krebs pointed out, the hack is “resource intensive” because it takes a lot of work to do some of this. For example to create a malicious false domain with the same information as in the victim’s network.

What this means is that certain “choice” organizations are such significant targets that the cyber thief dwells on ensuring they can rummage around (spy on emails for example) undetected.

There is no definitive proof I have seen that Russia perpetrated this hack. Why won't the media say that China or Iran or some other country could have done it?

Six years ago, another company

https://t.co/lzTINHgyAt

"Members of China's military systematically hacked the computers of SolarWorld USA, engaging in corporate espionage with the possible aim of advantaging SolarWorld's Chinese rivals, the US government alleges." (May 19, 2014)

"Chinese bank forced western companies to install malware-laced tax software

GoldenSpy backdoor trojan found in a Chinese bank's official tax software, which the bank has been forcing western companies to install." https://t.co/iEcdevXS7q

Another one from China: "execute files downloaded from a remote command and control (C&C) server, and update or uninstall itself." https://t.co/CpTRlx3n8h

They tell us China is the biggest threat to our security and then refuse to publicly say that China could have done it, instead reflexively naming Russia. https://t.co/4ZOhYgWT03

Even the official denials are well known! https://t.co/29Hd0wJilI

"A bombshell report claims that China has been developing a massive spying operation for a few years that involved building hardware backdoors into critical server components with the help of microchips no bigger than a grain of rice or the tip of a sharpened pencil."

"Those chips, once placed on motherboards that go into popular servers, would be able to help Chinese spies access information that would otherwise be unavailable to them."

"Secret Backdoor in Some Low-Priced Android Phones Sent Data to a Server in China"
https://t.co/MQoZ3XEtgc

"Pompeo warns governors of Chinese infiltration into US: 'It's happening in your state'" (February 2020)

https://t.co/inXsE8UxAl

IS THE SOLARWINDS HACK RELATED TO ELECTION INTERFERENCE AS SOMEONE SUGGESTED HERE ON TWITTER (sorry I can't find your tweet at the moment)

DID SOMEONE GAIN ACCESS TO THE STATES AND MESS WITH THEIR COMPUTERS SO THAT ELECTION DATA WAS SENT TO CHINA

THE REPORT ON FOREIGN ELECTION INTERFERENCE DROPS BY FRIDAY

Pompeo said to the governors: “The Chinese government has been methodical in the way it's analyzed our system... it's assessed our vulnerabilities and it's decided to exploit our freedoms, to gain an advantage over us at the federal level, the state level and the local level."

Pompeo warned them that we know.

“I'd be surprised if most of you in the audience had not been lobbied by the Chinese Communist Party directly."

“He said groups loyal to communist China are operating out in the open in Virginia, Minnesota, Florida and dozens of other states all around the country.”

“Other Chinese groups, however, practice their nefarious actions in the shadows in an attempt to exercise influence over U.S. citizens and lawmakers.”

Examples like “a diplomat from China, assigned here to the United States, a representative of the Chinese Communist Party, in New York City, sending a letter urging that an American elected official shouldn’t exercise his right to freedom of speech”

THEY ARE ATTACKING OUR CHILDRENS MINDS SAID POMPEO THROUGH THE SCHOOLS

“The secretary said ...that Chinese officials based in the U.S. are actively seeking to sow seeds of chaos at the state and local level -- specifically in the realm of education on college campuses and K-12 classrooms.”

“Maybe some of you have heard about the time when the Chinese consulate paid the UC San Diego students to protest the Dalai Lama. It shows depth. It shows systemization. It shows intent.”

WAKE UP WAKE UP WAKE UP REMEMBER CYNTHIA A JOHNSON PLAYING PING PONG IN DETROIT WITH THE CHINESE OFFICIAL

“Chinese Communist party officials, too, are cultivating relationships with county school boards and local politicians -- Often through what are known as 'Sister City Programs' ... This competition is well underway."

REMEMBER THE HARVARD PROFESSOR ARRESTED CHARLES LIEBER NANOTECHNOLOGY GOT PAID FROM “THOUSAND TALENTS PLAN”

“Pompeo also spoke about China's campaign to recruit U.S. scientists and academics to share vital secrets, in exchange for monetary gain through their ‘Thousand Talents Plan,’”

“a campaign that has already targeted scientists and professors on campuses such as Virginia Tech and Harvard and triggered investigations by the Department of Justice (DOJ).”

https://t.co/bozYbHtPqb

CHINA TURNS STUDENTS INTO SPIES

“He also explained how Beijing pressures Chinese students in the U.S. to keep an eye on their fellow countrymen and report back to the government about their activities.”

CHINA PROPAGANDA FLOODS KIDS MINDS AND THE AIRWAVES

“China’s propaganda starts even earlier than college. China has targeted K-12 schools around the world”

THE FAKE NEWS OWNERS DO BUSINESS WITH CHINA THAT AFFECTS OBJECTIVITY https://t.co/dnCgXIUOQg

“Pompeo then warned state governors about doing business with China and said it is common to indirectly finance communism without realizing it.”

“I want to urge vigilance on the local level too”

“I hope you will all take on board what I've said today. Don’t lose sight of the competition from China that's already present in your state. Let's all rise to the occasion and protect our security, our economy, indeed all that we hold dear."

@threadreaderapp unroll

@threader_app compile