Twitter Thread by Lesley Carhart



Lesley Carhart
@hacks4pancakes

Good morning to all of you well rested infosec folks who are just now waking up to this newest catastrophe :)

Fine, fine, I'll be nice. While you were sleeping, Google security notified of a long term (allegedly DPRK) SE campaign targeting infosec researchers on Twitter, ingratiating themselves into the community with minor research and blogs, then sending them malicious links and code.

The list of accounts is in the blog and 3 or 4 accounts were very active, messaged and drew in a ton of researchers, and successfully got some to execute malicious code in the name of exploit research. My thread is full of stories and screenshots. They hit a ton of people.

Here is the blog. https://t.co/T3No8Hj7xy

There are still a lot of unsubstantiated rumors and humble brags floating around about what else they did, so I would stick to the blog for now.

You need to check if you (or your team on work machines) interacted with any of these people, potentially followed malicious links, or amplified their social media posts.

@LawrenceAbrams also did not sleep: https://t.co/98UGrOk9fL

> North Korean hackers are targeting security researchers with malware, 0-days - @LawrenceAbramshttps://t.co/CkyMl6daoQ
>
> — BleepingComputer (@BleepinComputer) January 26, 2021

Anyway https://t.co/FNL9H3uZDh

> Am I doing this right? pic.twitter.com/MmxvYF6cJJ
>
> — fraggLe! (@fwaggle) January 26, 2021

Here is a particularly poignant and well documented one, as he discovers in real time what happened...
https://t.co/uibzAnNNUn

> Hey folks, story time. A guy going by the name James Willy approached me about help with a 0-day. After providing a writeup on root cause analysis I realized the visual studio project he gave me was backdoored.
>
> — Alejandro Caceres (@_hyp3ri0n) January 26, 2021

Anyway this is all novel not so much for the established sock accounts and Twitter SE (which *ahem* some researchers have been dealing with for ages ■■■■■■) but more because of the tactics of tricking exploit researchers into running malicious code, and burning a Chome 0day.

Good luck, all. VM all the things, and assume every inbound DM is gonna be a dickpic!

(This is also a very funny 5am joke because one of the fake people they used was named James Willy. Thank you, I have been here all night.)

