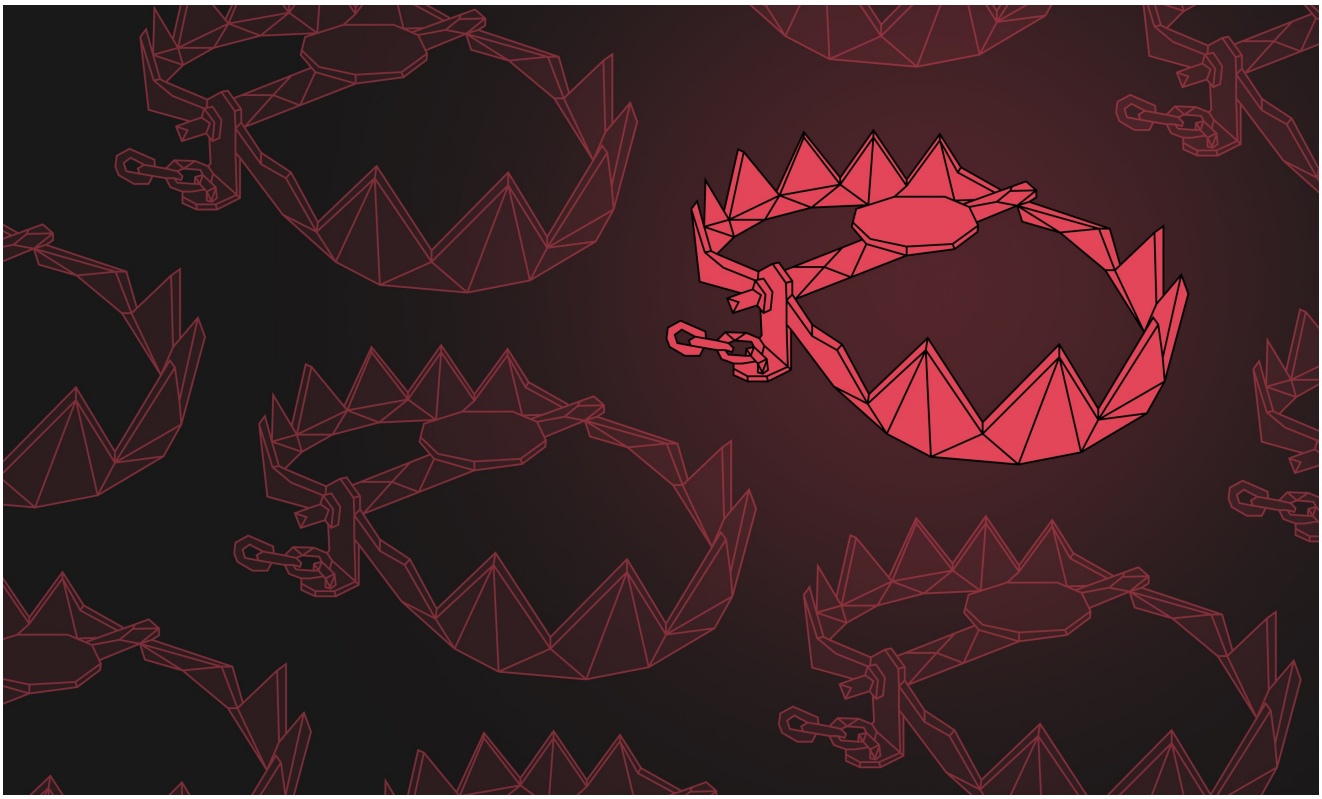
North Korea APT Might Have Used a Mobile 0day Too?

blog.zecops.com/vulnerabilities/north-korea-apt-might-have-used-a-mobile-0day-too/

By ZecOps Research Team January 26, 2021



Following Google TAG announcement that a few profiles on twitter, were part of an APT campaign targeting security Researchers. According to Google TAG, these threat actors are North Koreans and they had multiple goals of establishing credibility by publishing a well thought of blog posts as well as interacting with researchers via Direct Messages and lure them to download and run an infected Visual Studio project.

https://twitter.com/ihackbanme/status/1353870720191787010
Some of the fake profiles were: @z0x55g, @james0x40, @br0vvnn, @BrownSec3Labs

Using a Chrome 0day to infect clients?

In their post, Google TAG, mentioned that the attackers were able to pop a fully patched Windows box running Chrome.

From Google's post:

> In addition to targeting users via social engineering, we have also observed several cases where researchers have been compromised after visiting the actors' blog. In each of these cases, the researchers have followed a link on Twitter to a write-up hosted on blog.br0vvnn[.]io, and shortly thereafter, a malicious service was installed on the researcher's system and an in-memory backdoor would begin beaconing to an actor-owned command and control server. At the time of these visits, the victim systems were running fully patched and up-to-date Windows 10 and Chrome browser versions.

Attacking Mobile Users?

According to ZecOps Mobile Threat Intelligence, the same threat actor might have used an Android 0day too.

If you entered this blog from your Android or iOS devices – we would like to examine your device using ZecOps Mobile DFIR tool to gather additional evidence.
Please contact us as soon as convenient at

Hear the news first

- Only essential content
- New vulnerabilities & announcements
- News from ZecOps Research Team

We won't spam, pinky swear ✌
Follow @ZecOps