# EP 103: Cloud Hopper

darknetdiaries.com/episode/103/

cybercrime

incident response

26 October 2021 | 52:25

Full Transcript

Fabio Viggiani is an incident responder. In this episode he talks about the story when one of his clients were breached.

## Sponsors

Support for this show, and for stretched security teams, comes from SOC.OS. Too many security alerts means alert fatigue for under-resourced SecOps teams. Traditional tools aren't solving the problem. SOC.OS is the lightweight, cost-effective, and low-maintenance solution for your team. Centralise, enrich, and correlate your security alerts into manageable, prioritised clusters. Get started with an extended 3-month free trial at https://socos.io/darknet.

Support for this show comes from IT Pro TV. Get 65 hours of free training by visiting ITPro.tv/darknet. And use promo code DARKNET.

View all active sponsors.

## Sources

- https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper
- https://www.reuters.com/article/us-china-cyber-cloudhopper-companies-exc-idUSKCN1TR1D4
- https://www.fbi.gov/wanted/cyber/apt-10-group
- https://www.youtube.com/watch?v=277A09ON7mY
- https://www.wsj.com/articles/ghosts-in-the-clouds-inside-chinas-major-corporate-hack-11577729061
- https://www.technologyreview.com/2018/12/20/239760/chinese-hackers-allegedly-stole-data-of-more-than-100000-us-navy-personnel/

## Attribution

Darknet Diaries is created by Jack Rhysider.

Episode artwork by odibagas.

Audio cleanup by Proximity Sound.

Theme music created by Breakmaster Cylinder. Theme song available for listen and download at bandcamp. Or listen to it on Spotify.

## Equipment

Recording equipment used this episode was the Shure SM7B, Zoom Podtrak P4, Sony MDR7506 headphones, and Hindenburg audio editor.

## Embed Episode

Add this episode of Darknet Diaries to your own website with the following embed code:

```
<iframe frameborder="0" height="200" scrolling="no" src="https://playlist.megaphone.fm?e=ADV2735143955" width="100%"></iframe>
```

## Transcript

[START OF RECORDING]

JACK: Who's the person with the most power in the workplace? You might think it's the CEO or owner since they can call all the shots and make policy changes that everyone has to adhere to. But I think the most powerful person in the workplace might be the sysadmin, the

person who has administrative access to the core machines that are required for the business to operate. They can see what's in the database and they can read anyone's e-mail in the whole company, and they can see what files are on your computer, and they can sniff all the network traffic from your computer to see where you go and what you downloaded. Now, not every network is set up like this, where someone can see everything about everyone, and not all networks have one person who has all this access. But some networks are set up like this, where one person has control of everything. With the press of a button, they can bring business to a halt or potentially reroute customer payments or pay checks to them. It's crazy how much power they have.

Read Full Transcript

Previous Episode Next Episode