How To Hack an Optical Fiber in Minutes… And How You Can Secure It

November 17, 2016

Many people don't realize is that fiber optic cables are often easily accessible and unguarded, making them a potential target for hackers looking to tap into the huge amounts of data that travel across these fiber networks. Ciena's Paulina Gomez details the security vulnerabilities, while Patrick Scully gives a live demo of how easy it is to tap a fiber cable.
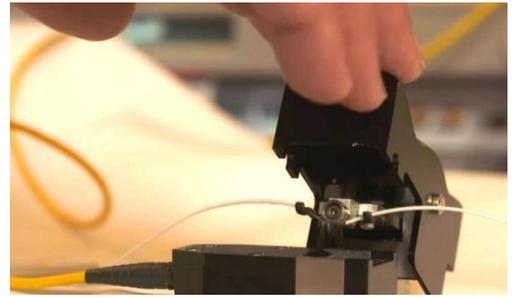
Have you ever set up a new smartphone? Changed your car's air filter? Then chances are you could tap a fiber line faster than it would take to install a new update on your iPhone. Think we're exaggerating? Keep reading or watch the video below.

According to a recent study (PDF), 37% of global companies are now deploying a consistent encryption strategy across their enterprise, as mega breaches and cyberattacks have increased companies' urgency to improve their security posture. With the increasing sophistication and frequency of data breaches—as well as the proliferation of diverse data centers and cloud services—no organization is immune to the ever-present threat of malicious attacks to collect sensitive and private information.

According to a recent study, 37% of global companies are now deploying a consistent encryption strategy across their enterprise, as mega breaches and cyberattacks have increased companies' urgency to improve their security posture.

But many of these encryption strategies are incomplete, focusing only on data that is "at rest" on company servers or in the cloud. Encrypting data "in-flight" between locations is critical as well.

Today, fiber optic cables are responsible for carrying enormous amounts of Internet traffic all over the world. Traditionally, the risk of fiber-optic cable intrusion has not been a priority consideration in most organizations' overall security strategy, although the threat of optical cable infiltration to access the data it carries is very real.

What many people don't realize is that fiber optic cables are often easily accessible and unguarded – even clearly marked with signs like the one pictured here to reduce accidental fiber cuts – making them susceptible targets for hackers.

Anyone with Internet access can shop online for one of several easy-to-get tools (like the one shown in the video below) and, after watching a few YouTube videos that guide you through the tapping process, be well-equipped to steal sensitive data from a fiber optic cable.

The worst part? Data breaches can happen on fiber without the provider even knowing that a breach has occurred. An operator may observe some loss on the optical line but will not know that his or her in-flight data is being monitored. This means that a network could be compromised for long periods of time without detection. Consider what this means when an optical fiber is carrying Terabits of unencrypted information – massive amounts of critical data can be collected for days, weeks, and even months.

Deploying an optical encryption solution, such as our award-winning Ciena WaveLogic Encryption, is the most effective means to protect against a fiber optic tap, as it protects all in-flight data, all the time, ensuring every bit is secure as it travels across the globe over any distance.

Whether supporting time-critical financial transactions, sensitive healthcare record storage, secure government communications, or simply wireless voice connections, today's networking infrastructure operates in an environment of ever-increasing threats. This is why securing data and the network is more important than ever. As increasingly sensitive information gets distributed across fiber-optic networks that span the globe, today's web-scale communications must deploy an IT security approach that encompasses not just server security and at-rest encryption, but also a robust in-flight optical encryption solution.