The Threat Stalkerware Poses to Your Business

Devolutions

INSTALLING SPYWARE PRESENTS A MASSIVE SECURITY RISK THAT EXTENDS FAR BEYOND A PRIVACY NIGHTMARE

Learn how installing spyware presents a massive security risk that extends far beyond a privacy nightmare – and how to protect yourself and your business.

A jealous spouse reads his wife's text messages, tracks her location, and downloads her photos without her knowledge or consent. A criminal installs a trojan on a victim's computer in order to steal their passwords. A company installs a tracker that monitors an employee's every click and keystroke.

Spyware – known also as stalkerware – has been around for quite a while. It comes in many forms, from simple tracking cookies to comprehensive surveillance software. Whatever form it takes, spyware is designed for one purpose: to allow the person who installed it to learn something about their victim with little regard for that victim's consent or privacy. Spyware is also widely available, easy to use, easy to install, and inexpensive.

In spite of all this, spyware is actually quite sophisticated. So perhaps it's not surprising that it has taken off in the consumer market. One of the alarming trends is that stalkerware has become tremendously popular amongst demestic abusers, and it appears with alarming frequency in cases of domestic violence. And even though it has been panned by cybersecurity firms such as Kaspersky, stalkerware shows no signs of going away anytime soon.

"Those peddling spouseware are willing to trade the agency of others for profit, considering some loss of life to be an acceptable cost of doing business," security expert Elle Armageddon recently told Vice. "Spyware is spyware, and it is a violation of the privacy rights of those targeted by it, regardless of whether they're dissidents being targeted by a state actor or [people] being targeted by their abusive partners."

But what does any of this have to do with your organization, exactly? Most would agree that it is unacceptable for stalkers, abusers, and governments to have access to tools that violate privacy. Still, does spyware (or stalkerware) really impact the business world?

Well, it's no secret that people are increasingly using their personal devices in the workplace. Imagine, for a moment, that someone connects to your corporate network on a device that's been compromised by stalkerware. Even if gaining access to sensitive data and corporate secrets was not part of the stalker's plan, it's important to remember that they see **everything** on the victim's device. At best, you're looking at potential issues with regulatory compliance. At worst, they might decide to make off with some sensitive documents for their own gain.

Granted, that second scenario is unlikely. But it's a good lead-in to my next point. Namely that businesses are every bit as vulnerable to stalkerware as individuals. After all, what better way to exfiltrate data from a corporate server than by covertly gaining someone's login details? And what better way to commit fraud than by monitoring the keystrokes of a financial analyst or a clinician? You get the idea.

So what can you do to protect yourself and your business?

- Pay attention to the applications you install and the files you download – particularly permissions on mobile apps. If an app requests permission you don't think it should have, uninstall it. It's not worth the risk.
- Install an antivirus and antimalware solution that's designed to track down and rid your devices of stalkerware alongside more traditional malware.

- Train yourself to recognize the warning signs of a phishing email or website.
- Enforce strict access controls on corporate-owned devices and a comprehensive acceptable-use policy for end-user devices.
- Familiarize yourself with the most popular stalkerware apps on the market.
- Pay attention to your devices and encourage your employees to do the same. Don't leave phones, laptops, or tablets unattended.
- Disallow jailbroken and rooted devices on your corporate network.

Stalkerware is a huge problem. Not just for privacy advocates or victims of abuse. For everyone. Follow the advice above and you should be able to better protect your business and employees.