Data Privacy Detective Podcast – Episode 8 – FBI CyberAlert about massive attack, July 25, 2017 – so what do we do?

Jul 28, 2017

Categories:

Blogs
Podcast
Publications
Technology Blog

Authors:

Joseph J. Dehner

The Alert lists about 200 domain names and IP addresses that individuals and businesses should avoid. The Alert lists four actions that all persons and businesses should take to avoid being harmed, not only by this attack, but to address the burgeoning rise of malware and other attacks against our data privacy and use of the internet:

- Have an incident response plan ready to implement if an attack occurs.
- Patch all web-connected systems against vulnerabilities. (Yes, it's worth the service provider cost!)
- Look carefully at the IP address and domain name of any unsolicited or unfamiliar email you receive, and never open an attachment from an unsolicited email without being sure it won't bite you!
- Block execution of malware in its unfolding variety of forms. (Be sure your provider protects you from current risks.)

To receive FBI reports about cybersecurity criminal attacks and become a better protector of your own data privacy and web connections, you can subscribe to the FBI's TLP:AMBER alerts. If you encounter suspicious or worse cyber-criminal activity, you should report it immediately at CyWatch@ic.fbi.gov or by phone at 855-292-3937. Let's join to counter threats to our privacy and the powerful positive force of the internet. Remember, your personal data privacy begins with you!

For more information, please contact Joe Dehner or any attorney in Frost Brown Todd's Privacy and Information Security Law Industry Group.