Hi, I'm Drew!

Welcome to my blog! It seems some introductions are in order. My name is Drew Newton. I am currently trying to start a new career in cybersecurity after spending 8 years in the service industry. I am starving for knowledge and am excited to share my research and findings on all things cybersecurity with everyone!

Check out my linkedin at the link above and say hi! I'd love to start a dialogue with anyone looking to discuss!

A Concerned Plea to Backup Your Data

ransomware, data, backup

Imagine that you receive a letter in the mail written in newspaper clippings informing you that all of the money in your possession is being held for ransom and the only way to get that money back is to allow the author of the letter to keep a fraction of the money. My impulse would be to spite that person and refuse to give up what is rightfully mine but then dinner time comes around and my fridge is all but empty and my stomach is aching and I'm almost out of toilet paper and my credit card payment hasn't cleared yet and it's almost the end of the month and I owe rent and… That initial spite has turned to panic as I try to navigate my life without all of the resources that I rely on day to day and you submit to the evildoers demands instead of starting your life from scratch. After all, what is an eighth of your earnings when you're left with nothing.

Everytime I see calls for companies to not pay ransomware demands to cyber threat actors, this scenario plays in my head. What are you supposed to do at that point? Logically, it makes sense that paying ransoms just incentivizes repeat attacks and sets a precedent for how companies will respond to these attacks but when your organization is losing more money as a result of not being able to access their infrastructure, how do you justify not taking the risk of paying the ransom.

The easiest and most logical work around in my mind is having backups of everything. It seems naive for any institution to assume that they are immune to these threats. My father is a pediatrician and even his small local practice has been the subject of a ransomware attack and small businesses have little to no recourse in these situations which means that script kiddies attacking smaller local businesses are almost guaranteed a pay day as long as their demands aren't too extreme. With how common ransomware attacks are every organization needs to understand the importance of backing up their data. There is no excuse not to.

Blog Posts

Last Pass Breach

password, manager, cryptography

I have used a password manager for five years at this point. Before that time, I reused the same password that I thought was so obscure that nobody would ever be able to guess it. It took multiple breaches from services that I had used and a quick search on haveibeenpwned to realize that my perception of online security was folly and my very obscure password was floating around the internet for anyone to use. In response, I put a lot of time into researching the most secure and user friendly password manager on the market which eventually led me to LastPass.

LastPass is one of the most widely used password managers currently available. When I was weighing my options, LastPass was the name that I saw the most. They market their service as "trusted by millions, recognized by experts" on their website and boast a local encryption service that utilizes the master password set by users as an encryption key to decrypt customers' password vaults. To someone who was not very cyber-literate at the time, this was enough to convince me (not to mention the service was free to use at the time). Going through the painstaking effort of changing the passwords for every account I could ever remember making, I decided I was a LastPass customer for life. Never would I have to go through this process again. That is, until last month when the details of a security breach that occurred at LastPass started to leak out to the public.

In December 2022 LastPass sent out a statement regarding a data breach that had been reported in late November. In this statement they announced that users' encrypted key vaults were in the hands of those responsible for the breach and that every user should consider their vaults as compromised and warned of incoming phishing schemes to try and obtain master passwords. These kind of attacks on services that boast security and store information as crucial as personal passwords are to be expected to a certain extent but the entire selling point of LastPass is that they have created safeguards for these very types of attacks. It's okay though, without a user's master password (which LastPass never receives and is only stored locally as an encryption key) the encrypted vaults are entirely useless, or so LastPass claims. They have done a great deal to take the emphasis off of the fact that a good amount of unencrypted data was also leaked along with the encrypted vaults such as personal identifiable information and usernames. This was like hitting the jackpot for a threat actor who can now take all of this PII and conduct a barrage of brute force, phishing and social engineering attacks on users.

LastPass has not followed up on this breach for a couple of weeks now and I can't help but feel like they're just waiting for this to all blow over. Meanwhile, anyone that put their trust in this company should be seriously considering mitigation strategies to keep their passwords safe. I, for one, will be here at home going through the painstaking effort of changing passwords for every account I could ever remember making on a new password manager once again.