ENJOY SAFER TECHNOLOGY®

THE ART OF LOSING (YOUR DATA)

www.eset.com

The art of losing (your data)

By Michael Aguilar, Business Product Technical Lead, ESET North America

Netflix. Target. LinkedIn. MySpace. Company brands that we are all familiar with. And they all have one thing in common: data loss due to breaches in the company's security. Some attacks were a result of malware—others, the result of a direct attack on the business. Stolen data containing sensitive or personal information from such attacks is typically then sold on the black market or various underground forums for cash. The amount requested for these credentials is not very expensive either, with *Lavasoft reporting* that 100,000 LinkedIn user logins sold for a mere $2,000 in Bitcoins, or just about $.00002 per account. So how do you protect sensitive data that your business has built up, and keep your customers safe from a breach? For that matter, what can you do to best protect your own data?

Hacks and attacks

In 2012, LinkedIn servers were hacked by Russian cybercriminals, and credential sets were stolen (more info *here*). The passwords were hashed; however, they proved to be vulnerable to cracking and were eventually released online. LinkedIn advised its users to change passwords and enable two-factor authentication (2FA). Fast forward to 2016, and yet more passwords were leaked online pertaining to the original data breach in 2012. Users again were advised to change their passwords and to enable 2FA on their accounts.

Another issue began around this time. People with TeamViewer and PayPal accounts began to notice odd behavior. Some PayPal users noticed that PayPal had transferred all of their funds to an overseas account, while some TeamViewer users noticed that their machines began to control themselves, eventually asking for funds to stop the behavior. Then, in a perfect storm scenario, the TeamViewer service went dark on June 1, 2016, due to a domain name system issue. These hacks and attacks catch users off-guard, and leave a dim outlook on what to do next. When it comes to odd behaviors surrounding YOUR personal information, there are proactive steps you can take to stay safe online. Follow the steps below to win at the art of protecting, not losing, your data.

Proactive steps

1. **Never re-use password across multiple sites**
   Nearly all of the "affected" clients that TeamViewer analyzed had re-used credentials across multiple sites, including LinkedIn, MySpace and others that had recently suffered a data breach. By re-using a

credential, it allows attackers to determine if your credentials are valid at any other sites in an automated fashion. So those credentials that you used to sign up for MySpace to broadcast that awesome 2005 playlist were also used to drain your PayPal account. If, for some unknown reason, a credential must be used over multiple sites, the best recommendation is to enable their two-factor authentication systems, if available—though the fundamental warning and advice remain firmly the same: Do not re-use the same password. Also, to aid with the memorization of a plethora of passwords and assist in creation of hard-to-break passwords, you can use a password manager like *LastPass*. It helps you create secured passwords, audits them and works much better than a sticky note.

2. Check your accounts regularly

Another lesson that can be learned from these large-scale breaches is to be aware of your accounts and to check in on them from time to time. I have had many, many user accounts over my digital life, and have abandoned a number of them over time—some, many years ago. Trying to check each one individually is time-consuming and almost always fruitless. Have I Been Pwned? is a great resource to check if your account has been compromised in a data breach. Data is aggregated from company breaches and makes its way to "paste" sites like Pastebin,

which stores online text for easy sharing. Have I Been Pwned? allows you to enter your email or usernames and determines if you were part of a data breach. The site can check against breaches concerning some of the most–used companies, like LinkedIn, MySpace, Avast and Adobe. Checking just one of my personal email addresses yielded four sites I had visited only a few times that had been compromised. You also have the availability to be notified if a credential you use becomes part of the public domain. And if any of you do have my MySpace password, I'm sorry—the music selections were horrible. Also, Tom never friended me, so there's that …

3. Take advantage of enterprise protections

Companies can stay on top of securing data by using a data loss protection (DLP) application like Safetica. DLPs ensure that data is appropriately used for work purposes and that nothing is misused or distributed. The application keeps malicious activity at bay, including the copying of data to a thumb drive; hacker activity; and non-standard user transfer of files off-network (presumably to sell). Agents installed on machines catalog the type of data being transferred and the applications being used, and applies rules that are created and configured to identify suspicious activity. So, for example, in the instance that these agents see an account named "haxor" sending files to a remote location or notice that someone is copying massive amounts of financial or sensitive documents when they should not be, you'll be notified to take action before the information hits the public domain. Safetica also allows the option to block websites and devices to help mitigate risks. Their agents are very lightweight, and I have noticed no performance hits while using the application. The amount of data gathered is also pretty neat, considering generated reporting is direct and to the point. If you are looking for malicious data activity, DLP applications are your best friends.

What should you do if you've been compromised?

If you have been part of a data breach and your personal information was leaked, there are actions that you can take. Normally, large businesses are good about offering some form of credit-monitoring or data-monitoring service for free if you were part of a data breach. When Experian was hit with a data breach in 2015 that affected T-Mobile users, credit- and identity-monitoring services were offered free of charge for two years to ensure that no oddities occurred as a result of their security breach. When the Office of Personnel Management for the U.S. government was affected by a data breach, it offered identity-monitoring, credit-monitoring, and identity-restoration services; identity theft insurance; and even access

to a virtual browser to protect you during online transactions. Similarly, *ESET's banking and payment protection* uses a secured browser to allow you to conduct online transactions safely. Target paid back victims of its data breach; however, it only implemented more smart card systems, or "chip-and-PIN" card systems, at the point of sale, and did not offer the free monitoring services that some companies have when their data was leaked.

With our increasingly interconnected digital lives, it is difficult to keep watch over all the data that we have created. But with a bit of diligence and some proactive thinking, you can greatly reduce the risk of your credentials being used against you. It's worth doing, because the risk is very real. After all, if it can happen to me, it can happen to anyone.

Michael Aguilar is a business product technical lead at ESET North America. He is studying for the CISSP exam and has a Security+ certification as well as a Usable Security certification from the University of Maryland Cyber Security Center via Coursera.org. He is currently responsible for working with large-scale clients for ESET North America and works with ESET developers, QA, and support engineers to resolve issues with clients in a quick and effective manner. Michael is active on Spiceworks and various security forums looking at new threat vectors and the best controls to mitigate those risks.

For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit www.eset.com.

ENJOY SAFER TECHNOLOGY®