Week 1: October 1 - October 10, 2015
Two-factor Authentication

Two Factor Authentication

Traditional Passwords No Longer Work

In many cases an online password is what separates the average person from financial or reputational harm. Despite their flaws, they are the way we authenticate into our online lives: e-mail, banking, social media, cloud data storage, and so much more. Of all the cyber adversaries the FBI pursues, all incorporate some form of credential theft to maximize exploitation. From cyber espionage campaigns, hacktivism, and criminal malware campaigns, credential theft has become a central focus to the cyber adversary – as in some cases they yield the "keys to the kingdom," or very valuable and/or marketable data.

As processing systems and technology increase, so does the ability for attackers to obtain credentials through technical means (brute force, dictionary, keylogger), or non-technical means (password guessing, defeating accounting security questions). Social engineering is one of the primary avenues of credential compromise. With a well-crafted message and easily spoofed webpage, passwords can be obtained by the least sophisticated means necessary.

Traditional passwords rely on one factor: something you know. For simplicity sake, and in an effort to remember a password, users:

- Minimize the size and complexity of their password
- Standardize passwords amongst online accounts
- Do not change passwords over time, leaving them static

This all lowers the bar for the cyber thief, and leaves users susceptible to compromise.

Impact of Password Compromise

E-mail is one of our primary means of communication from both a business and personal standpoint; all your e-mail and contacts with others (including attachments) may be exposed to the public now or in the future. E-mail accounts are frequently associated with and used for other online services, including: bank websites, social media, travel websites, online backup or cloud storage sites. These accounts are associated with personal e-mail accounts as both a means of identification and authentication. If an e-mail account is compromised, in addition to the privacy breach, threat actors gain an additional trusted platform to attack other accounts. The end result could lead to embarrassment, identify theft, and financial fraud and theft.

Two Factor Authentication

Multi-factor authentication increases security by incorporating requirements beyond something you know. When two factors are required to authenticate, this is known as two-factor authentication (TFA). TFA can include a combination of:

- Something you know (a password/passphrase)
- Something you have (a dynamic token or pin)
- Something you are (biometrics)
- Someplace you are (location at time of authentication)

Combating Credential Theft

For most home Internet users, TFA is available **as a free service** by utilizing something you know and something you have. Many e-mail service providers, social media platforms, cloud bases storage solutions, and even banking and finance sites have made TFA available to users by requiring a strong password, and provide a pin that changes at a set interval (many times between one to two minutes). Users can receive those pins very easily through a text message or a mobile application. This does not mitigate the need for strong passwords, as users should endeavor to make difficult all efforts to steal credentials by cyber adversaries.

If a cyber threat actor employs technical tools to compromise your password, or obtains it through social engineering, it is much more difficult to compromise your account (and in turn other online accounts) as they do not have access to the changing pin. Although the extra step takes a bit more time for the end user, the benefits from a security standpoint cannot be overemphasized. After a compromise, the combined effort to regain access to personal accounts, fix credit, to chase money, or to suffer the loss of personal data, can far exceed that of adding a step to authenticate.

Business Implications

Many large businesses have recognized the benefits of deploying MFA to the workforce, and in so doing have dramatically decreased the risk of credential theft and the subsequent loss of sensitive or proprietary data. Many small to medium businesses have not deployed MFA, or utilize web-based e-mail as a means of communication.

Education campaigns by employers can breed awareness amongst employees on the importance of utilizing strong passwords, and when applicable, free TFA services on personal accounts. While some employers maintain policies which prohibit the use of personal e-mail for business purposes, for a variety of reasons employees still do work through personal accounts. Those reasons may include: regular access to personal e-mail on mobile devices, bypassing corporate e-mail restrictions on file attachment type or size, maintaining work documents “in the cloud” for access anywhere, etc. By

educating employees on the importance of TFA, corporations may not only protect the employee, but the organization as well.

Within the organization, TFA reduces the likelihood of system and network compromise when utilized by those with privileged access (such as executives and network administrators). Threat actors can do the most damage when they compromise the network and obtain privileged credentials. By obtaining these credentials, it dramatically increases access to the system and network, and in turn significantly drives up the cost of mitigation efforts.