The Impacts of Compromised Credentials

Introduction

The password has always been a long, sought after target of the Cyberattacker. But given today's Cybersecurity threat landscape – they are after much more than just that. For example, they not only want to know more about you, but they want to come after you and literally take everything that identifies you. It is challenging to know even you are a victim until it is too late.

One of the biggest reasons for this is that the Cyberattacker is taking their own time to find and research their unsuspecting victims. For example, they are not interested in finding targets en masse, but rather, they are now interested in selecting just a few and finding their weakest spots. Then, once they penetrate in, the goal is to stay in as long as possible and steal as much as they can in small bits, going unnoticed.

The Types of Attacks

There are three types of credential theft, which are as follows:

1) Against the individual:

   This when one particular individual or even a group of them are selectively targeted. In this instance, the attack vectors may not be too sophisticated in nature. For example, Phishing based Emails are still the favored weapon of choice. Despite all of the publicity and notoriety that it gets, people still fall for phishing schemes. It can come in one of two ways:

   - The victim can be duped into clicking onto a malicious link. Typically, the link that is in the body of the Email message is different than when you hover your mouse pointer over it. But even this has changed. The two links now appear to be almost the same, thus tricking the victim even more. From here, he or she is then directed to a spoofed website that looks so legitimate and authentic that it is almost impossible to tell that it is really a fake one. From here, the victim then enters their username and password, and the havoc starts.
   - The victim can also be duped into downloading a malicious document. The most favored file extensions used here are that of the .DOC, . XLS, . PPT, and .PDF. Once any of these attachments are downloaded and opened up, the malware spreads into the victim's device, in an attempt to steal as many credentials as possible. An excellent example of this is keylogging malware. The keystrokes are recorded and covertly sent back to the Cyberattacker, in an effort to ascertain all of the credentials that the victim uses. This has also become rather sophisticated in nature, as the hijacking of the contact list is now commonly used, making it look like that Phishing Email has been sent by a person that the victim knows well.

2) Against the business:

   This is technically known as "Corporate Credential Theft." In these instances, the Cyberattacker has much more at their disposal in which to harvest as many credentials from victims as they can. For example, many companies in their digital marketing efforts, very often use Social

Media, such as Facebook, Linked In, and Twitter. Although the communications may be careful in what they post about their company, the Cyberattacker can still glean quite a bit off of it. Over time, they can see those employees that post material regularly, and the timeframes that they do so. From here, they can narrow down their list to just a few potential victims and study them even more carefully through their social media activity. In other words, the Cyberattacker is building up a profile of their victim that can be used to determine their vulnerabilities, even with publicly available information. A commonly used threat vector is that of the Business Email Compromise (BEC). This is where an email is sent, or even a Social Engineering based phone call is made purporting to be the CEO and asking his or her administrative assistant to wire a large sum of money to a bank account, which, of course, is located offshore. Once the money has been transferred, and the mistake has been noticed, it is very difficult to get the money back or even trace down who launched this sort of attack vector.

3) Credential Abuse:

This is the ultimate goal of any compromised credential attack. Once all of the credentials have been harvested to the greatest amount possible, the Cyberattacker will then use them for credit card theft/fraud, hijacking money from banking and other types of financial accounts, and worst yet, launch long term Identity Theft attacks. But there are two new trends that are occurring in this regard, which are:

- The Dark Web: The Cyberattacker can sell these credentials here for a rather nice profit.
- Lateral Movement: In this instance, the Cyberattacker will use their hijacked credentials in order to infiltrate the network infrastructure of a business, and from there, move in deeper in a "sideways" fashion in an attempt to find even higher-value targets, such as those of Intellectual Property (IP) and other mission-critical digital assets. The time that the Cyberattacker resides is very often referred to as the "Dwell Time," and given just how sophisticated they have become, they can stay in for weeks and even months without ever getting noticed.

How To Prevent Compromised Credential Attacks

This is a serious problem, as according to the Verizon 2020 Data Breach Investigations Report (DBIR), over 80% of the hacking attacks that take place make use of heisted or stolen credentials. Further, at least 77% of the Cloud security breaches also involve the use of hijacked credentials.

(SOURCES: 1 and 2).

In the end, probably the best line of defense that you can use is what is known as the "Zero Trust Framework." This is a methodology which stipulates that you cannot, under any circumstance, trust anybody internal or external to your company when it comes to accessing shared resources. Anybody wishing to have this kind of access must be authenticated through at least three or more layers of authentication at each line of defense.

Sources

1) https://securityboulevard.com/2020/06/credential-vulnerabilities-most-likely-breach-culprit-verizon-dbir/

2) https://thycotic.com/company/blog/2020/06/17/verizon-2020-dbir-5-top-takeaways/