INSIDER THREATS-GROWING MORE DANGEROUS

BY JAY BORDEN

Insider threats have long been a risk. Why, because employees and executives already have access to your systems, applications, and data. Many of them to highly private and confidential information such as strategy, intellectual property, customer, client, or patient private information.

But how do insider threats play into this? Two ways, intentionally and unintentionally.

Let's begin with intentionally. If an employee is unhappy or worse, disgruntled, they may want to get back at their employer. They can choose to steal information and sell it, or they may be susceptible to offers to steal data. The offers may come from competitors or attackers. Foreign nationals may be targeted because they often have relatives in another country that can be threatened. The employee may just want to inflict damage on their employer to get back at them for something.

Now let's look at the unintentional category. This has two branches, compromised and naïve and both difficult to defend against. The compromised category refers to people who were compromised unknowingly and bring that compromise to work. The compromise may have happened at work while going to websites or doing social media, etc. Or it may have occurred at home while surfing, shopping, gaming, or anything else. Nonetheless, there is malware on the device and their credentials are for sale. The compromised credentials may include those for work.

Naïve people simply don't understand basic cyber hygiene and follow risky practices thereby putting their company at risk.

Whatever the motivator, it can be difficult to detect their theft or damage because their role grants them access to the systems and information.

INSIDER THREATS-GROWING MORE DANGEROUS

CONTINUED

How do attackers gain access? Many ways. Phishing is one of the biggest attack channels. The email that looks like it came from a legitimate source and asked for information to prove identity may well be from a cybercriminal and steal your credentials. The variation on phishing called smishing is the use of text messages to steal information and vising, the use of voice messages to do it are all very effective.

How effective? One Brightly Cyber accesses the largest repository of recaptured credentials with over 766 Billion recaptured assets. That breaks down to 1.7 billion malware records, 33 billion passwords, and 39 billion email addresses. There is much PII, Personally Identifiable Information, such as home address, Social Security Number, and more recaptured but not included in these counts.

Yes, there are some duplicates that come from different sources but that is still an enormous number of credentials out there.

Other ways attackers capture your credentials are if you search for free copies of software or games or game cheat codes. You may get what you want but be sure it comes with malware installed.

But you run a well-known anti-malware package. and your company uses endpoint detection and response. Why don't they work? They do work and protect against a lot of things. However, 66% of the infostealer infected devices found also used those protections.

Cybercriminals constantly improve their attacks to avoid detection. A phishing message may send you to a malware infected site that downloads the malware in the information you want.

In other cases, the site it sends you to is clean and the protective software allows you to go. But that site redirects you to an infected site that the protective software doesn't see.

Another way information gets compromised is by the reuse of passwords, using the same password for more than one system or site. If attackers get a password, they will try it in many places. That is called password stuffing, and it is very effective.

INSIDER THREATS-GROWING MORE DANGEROUS

CONTINUED

What if you use a home computer to log into office systems? Do your children or other family members use that computer? Are all the sites anyone visits for personal use safe? Difficult to tell but chances are high they are not. If malware came from one of those sites it will steal credentials to access your other personal and business systems.

Malware has improved significantly over the last few years. It is now very good at evading protective software. Once installed it will find ways to disable the protections and then spread across the environment, escalate its privileges to gain better access to information, and more.

Some malware variants steal information, create a backdoor allowing future access, then delete themselves. Protective software can't find what is no longer there. But what the information attackers want is already gone. They will return often through the backdoor to get anything new.

Another key target is cookies. The number of cookies stolen is way higher than the number of passwords because the number of cookies on your devices is so much higher than the number of passwords.

Cookies are being used to build a picture of the user. Then use it to steal more information or access other systems.

Regardless of their category or how they were infected, the entire company is at risk.

Visit our website onebrightlycyber.com or call (888) 873-1920 to learn all the ways we help keep you safer.