Understanding the Dark Web and Protecting Your Property

by Andrew Cardno

One of the most popular pieces of jargon that gets thrown around in cyber security discussions is the existence of the Dark Web, a mysterious place wherein all kinds of nefarious dealings occur, where anything can be found and bought. To help demystify the Dark Web, let's start with what it actually is. The Dark Web refers to a specific part of the internet that is in a secret network. It should not to be confused with the term Deep Web, which refers to all parts of the internet that are not indexed. Technically speaking, the Dark Web is a part of the internet that is highly encrypted and can typically only be accessed through a browser such as Tor. The nature of the Dark Web means that anything and everything is anonymous, transactions are conducted in cryptocurrency, and it is near impossible to trace an IP address or get a geolocation on someone. This makes it the ideal marketplace for criminal transactions, often involving drugs, weapons, or other contraband. While it is the case that the Dark Web is comprised of criminal activity, approximately 57%, it also attracts lawful business due to the anonymous nature of its' services and websites. For example, ProPublica and Facebook have set up sites that can only be accessed via a Tor browser. However, from a casino's perspective, the most important thing to understand about the Dark Web is that it sells information, including bank accounts, remote desktop computer access, credit cards – really anything that hackers can get their hands on.

Potential Breach

Consider this scenario – you are a midsize casino with a thriving operation, and you decide as a company to expand your property. There are a lot of things that go into undertaking such a venture, but one thing that a casino might choose to do is to set up a remote desktop environment so that your systems contractor can assist you in the install from a distance, and in doing so it is possible that you let that environment open up to the internet as a whole. What you might not know is that by doing so, you expose this environment to significant risk as hackers are constantly scanning the internet looking for anything that accepts a remote desktop protocol (RDP) connection, and subsequently attempting to break into it. Once that is done, they can place access to the environment on a marketplace where anyone can purchase the credentials, and once they have accessed the environment, attempt to move into other places within the network. While this kind of attack is random and relatively easy to defend against, by disabling access to the open internet for your RDP connections, among other things, there are all kinds of ways in which your business can be compromised via the Dark Web.

You Don't Know What You Don't Know

In many cases it can take years for a breach in security to be noticed, in part because the Dark Web can be a fickle place. Websites move or shut down, Distributed Denial of Services attacks render sites unusable, and sometimes things just do not sell, and as a result, this information on your company, or even your employees can sit there for months or years. All it takes is one phishing scam that was too convincing or one employee whose password was too easy to guess and suddenly your casino is compromised and you do not know about it. It is entirely possible that nothing ever comes of this breach, your employee might move on before their information is used, or the password to a compromised system might be changed as a part of your standard routine. It is entirely possible that access to your company might already be available on the Dark Web.

Going Bigger

So you might be asking yourself what the big picture here is – if your company is already compromised what can you do about it? Well the first thing is easy, arm yourself with knowledge about what the Dark Web is and what kind of activity takes place there. This will go a long way in preparing your business for a potential breach. The next step is hire professionals to help you. There are people and companies out there that are already prepared with the necessary tools to help your business with identity theft protection, dark web monitoring, and infiltration testing. All of these are essential parts of the puzzle to help protect from breaches and to clean up after they have happened. You should also communicate with your employees through this entire process as they are the keys to the security of your networks. It only takes one access point for a network breach, but if all of your business works as a team, then you don't have to give even one access point to hackers.

The Dark Web is a scary place for businesses to think about, but by arming your business and employees with the right knowledge and tools, it becomes possible to defend against the Dark Web's bad actors. ♣

Andrew Cardno is CEO & Founder of Innovation Gaming Group. He can be reached by calling (858) 254-0412 or email andrew.cardno@innovationgaminggroup.com.