HOME CYBER DEFENSE

ARE YOU SAFE FROM CYBER CRIME?

WEEKLY

Volume #4 - Issue #181
October 12th, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

What Is Doxing

With the arrest of a congressional staffer for posting the personal information of several Republicans online, we thought this is a good opportunity to explain Doxing, and why it is a crime.

In one of the biggest examples of doxing, a hacker released the personal information of 29,000 federal employees – twenty thousand from the Department of Justice and 9,000 from Homeland Security – which included names, job titles, phone numbers, and email addresses. Incidents like this, including the doxing of CIA director John Brennan by a hacktivism collective, prompted the FBI to issue a warning to law enforcement and high-profile public officials indicating they could be targeted by hacktivists, who have increasingly adopted doxing as a form of social justice. The advisory notes that such doxing attacks are likely to continue with possible targeting of family members, and urges officers and public figures to be vigilant about their social media activities and password security.

The prevalence of personal information online, as well as users' propensity to over-share through social media has led to an increase in 'doxing' – the process of gathering and posting an individual's personal information without his or her permission. This information can include names, ages, emails, addresses, phone numbers, photographs, and his or her overall pattern of life, all of which can be found via publicly available sources. While doxing is nothing new, the proliferation of social media has aided in it becoming a common tactic for of harassment, especially towards high-profile individuals. Using the right techniques and sources, including search engines, social networking sites, and data aggregators, threat actors no longer need complex social engineering schemes or malware attacks to get the information they want about their targets. Instead, they can determine a wealth of personal information on executives and their family members by examining their online footprints.

While some individuals perform doxing out of general curiosity about a person or company, others have more nefarious motives. This includes revenge, extortion, or embarrassment, all of which can be achieved by exposing the sensitive information that they have gathered about the person or company. If the doxed information includes a person's social activities, medical history, sexual preference, or other private information, there could be a serious threat to the health, livelihood, and career of the target.

Often doxing does not only affect the targeted individual, but also their families, including the names and ages of children, school, and spousal information. This is seen with leaders of large corporations and politicians that support controversial issues. This information is typically posted to anonymous data-pasting sites such as Pastebin, which makes determining who posted the data nearly impossible.

Hacktivists have increasingly adopted doxing as a form of social justice. In 2015, vigilantes and hacktivists doxed Walter Palmer, the Minnesota dentist who shot Cecil the lion; Brian Encinia, the Texas police officer who arrested Sandra Bland; and more than 300 employees of Planned Parenthood. Hacktivists even attempted to dox the leaders of the Islamic State. All of these incidents were a direct reaction to public event where individuals feel that a social issue was violated.

Strictly speaking, the legality of doxing has not been universally established. Some states have moved to criminalize doxing under certain circumstances, specifically if the threat actor outlines the physical location of any individual and voices the intent to harm, shame, stalk, humiliate, endanger, or otherwise compromise the safety and security of said target. These states argue that the person is in a position of risk and the threat actor is likely in violation of state-level stalking laws.

Probably one of the most dangerous business orientated sites for doxing is LinkedIn. Be very careful about the information you put in your profile, what you post on the site, the connections you make, questions you answer about your business, and attachments you open from your LinkedIn site or emails sent to you from LinkedIn connections.

Thank you for subscribing to our email!

Home Cyber Defense Weekly

is a service of

House of File Technologies