Thwarting hacks by thinking like the humans behind them

February 5 2020

Credit: CC0 Public Domain

If we understood the humans behind hacking incidents—and their intent—could we stop them? Research from Michigan State University reveals the importance of factoring in a hacker's motive for predicting,

identifying and preventing cyberattacks.

Most people tend to focus on how to minimize the risk of a hack, from antivirus software to regularly updating computer software. While these defenses against attacks are helpful, study author and MSU criminal justice professor Thomas Holt believes it's just as important to have a strong offense.

"The more we start thinking like an attacker, the more we can better secure systems and move away from this perspective that everything can be solved through a piece of software," Holt said. "Any good attacker, no matter what their motivation is, can get around a security tool."

Holt found that the targeting practices of a specific kind of hack called a web defacement—where the attacker changes the original content of a webpage to images or content of their choosing—vary based on the self-identified motivation of the attacker.

"Their decision-making process can be modeled, and it can help us to understand how to better secure systems and think like a hacker," Holt said.

While considered a simple form of hacking, web defacements are a timely concern, Holt said.

"Earlier in January, hackers claiming ties to Iran defaced a U.S. government website. The page for the Federal Depository Library Program was replaced with pro-Iran messaging and an image of a bloodied President Donald Trump," Holt said. "The defacement demonstrates hackers are motivated by more than money, and that they may engage in future cyberattacks."

Holt collaborated with Rutger Leukfeldt and Steve Van De Weijer from

the Netherlands Institute for the Study of Crime and Law Enforcement to analyze more than 100,000 web defacements against websites from January 2011 to April 2017. The researchers wanted to see if the targets of defacements were associated with attacker motivation, and how they actually performed the hack as well.

The findings revealed that web defacements—one of the more public forms of hacking—can be inspired by a variety of motives. The ways a defacement can be performed also vary, though defacers often attempt to compromise as many sites as possible as quickly as possible. Targeting thousands of web pages simultaneously demonstrates more skill as a hacker than if only one is targeted, unless it is a high level, recognizable site.

"If you can demonstrate to others your capacity, or expertise, that has value," Holt said. "So people will begin to realize and connect the handle or online nickname you use with some type of skill. It can net you clout within the hacker subculture. When you use more sophisticated methods or do things in a novel way, that lends an air of credibility to your identity."

Due to the overall threat they pose, hackers engaging in data breaches or using ransomware garner more attention than those acting out of subcultural or ideological motivations. Still, examining all types of hacks—and the hackers behind them—will help researchers predict and defend against cyberattacks.

"We can't just say we're only concerned about the economic stuff," Holt said. "We have to be concerned about political, ideological and subcultural at the same time."

More information: Thomas J. Holt et al. An Examination of Motivation and Routine Activity Theory to Account for Cyberattacks

Against Dutch Web Sites. *Criminal Justice and Behavior*. First Published January 19, 2020. doi.org/10.1177/0093854819900322