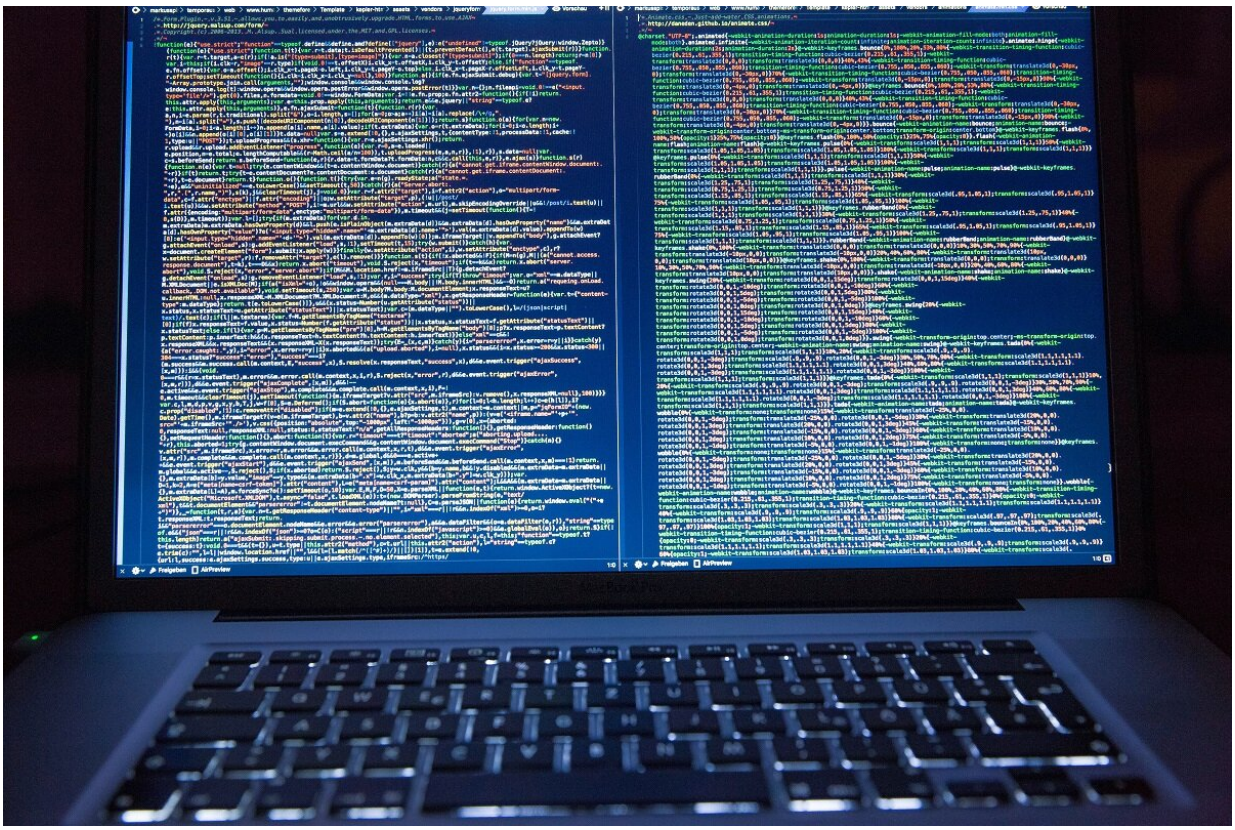
Defending against cyberattacks by giving attackers 'false hope'

January 28 2019, by Eric Stann



Prasad Calyam and researchers at the University of Missouri hope to employ a new strategy in the ongoing struggle to protect digital information in the cloud from targeted cyberattacks. The strategy establishes a new artificial intelligence system to combat digital intrusions. Credit: University of Missouri-Columbia

With almost every online purchase, a person's personal

information—name, date of birth and credit card number—is stored electronically often in the "cloud," which is a network of internet servers. Now, as more people buy from online businesses, researchers at the University of Missouri hope to employ a new strategy in the ongoing struggle to protect digital information in the cloud from targeted cyberattacks. The strategy establishes a new artificial intelligence system to combat digital intrusions.

"We are interested in the targeted attacks where the attacker is trying to exploit data or critical infrastructure resources, such as blocking data access, tampering facts or stealing data," said Prasad Calyam, associate professor of electrical engineering and computer science and the director of Cyber Education and Research Initiative in the MU College of Engineering. "Attackers are trying to use peoples' compromised resources to infiltrate their data without their knowledge, and these attacks are becoming increasingly significant because attackers are realizing they can make money in a big way like never before."

In this study, the researchers focused on two types of cyberattacks—those seeking customer data and those stealing resources such as bitcoins, a type of digital currency. Their strategy uses artificial intelligence techniques and psychology principles—giving the cyberattacker false hope that the attack is working.

"Our 'defense by pretense' system quarantines the attacker and allows the cloud operators to buy time and build a stronger defense for their systems," Calyam said. "The quarantine is a decoy that behaves very similar to the real compromised target to keep the attacker assuming that the attack is still succeeding. In a typical cyberattack the more deeply attackers go in the system, the more they have the ability to go many directions. It becomes like a Whack-A-Mole game for those defending the system. Our strategy simply changes the game, but makes the attackers think they are being successful."

Researchers say buying time is important because it allows those directing the cyber resources to devise a more sophisticated defensive strategy to use at a later time when the cyber-attacker returns to make a more vigorous attack knowing that valuable assets are being defended.

The study "Intelligent defense using pretense against targeted attacks in cloud platforms," was published in *Future Generation Computer Systems*.

More information: Roshan Lal Neupane et al, Intelligent defense using pretense against targeted attacks in cloud platforms, *Future Generation Computer Systems* (2018). DOI: 10.1016/j.future.2018.10.004

Provided by University of Missouri-Columbia