Computer hackers could be thwarted by new 'deception consistency' method

November 28 2018

Hack attack. Wikipedia, CC BY-SA

Can you deceive a deceiver? That's the question that computer scientists at Binghamton University, State University of New York have recently been exploring.

Assistant Professor of Computer Science Guanhua Yan and Ph.D. student Zhan Shu are looking at how to make cyber deception a more effective tool against malicious hackers.

Their study was inspired by the 2013 Target data breach that affected 41 million consumers and cost Target $18.5 million, and the 2017 Equifax hack which exposed the personal information of 147.7 million Americans. Both of these were what can be classified as Advanced Persistent Threats (APTs).

Yan and Shu wanted to improve the ways in which hackers are countered when attempting APTs, so they focused on refining existing cyber deception tools.

Cyber deception is a responsive technique that puts malicious hackers into a fake environment once the system detects a hack in progress.

In the abstract of the study, the researchers wrote that "the main objective of our work is to ensure deception consistency: when the attackers are trapped, they can only make observations that are consistent with what they have seen already so that they cannot recognize the deceptive environment."

They found that this focus on only showing attackers what has been seen before increases the efficiency of the deception.

"The issue is that sometimes cyber deception uses what are called 'bad lies' that are easily recognizable by the attacker. Once the deception is realized, the attacker can adjust and work around this form of protection," said Yan.

The deception consistency method that Yan and Shu created was tested on college students who had recently completed a cybersecurity course.

The students were asked to act like malicious hackers, with some ending up in the deceptive environment.

The researchers found that because the deceptive environment was consistent with what students had previously seen, most did not realize they had entered into the deception.

"It was clear that most students were simply guessing whether they had entered into the deceptive environment or not. They couldn't quite tell the difference when we used our consistent model," said Yan.

Although the deception consistency may make it more difficult for APT attackers to recognize the deception, the researchers were clear that their proposed method is not a cure-all for things like what happened to Target and Equifax.

"It may not hold up against more advanced attacks, but we will continue to improve the effectiveness of the deception-based methods against a variety of attack scenarios," said Yan.

Yan and Shu published "Ensuring Deception Consistency for FTP Services Hardened against Advanced Persistent Threats" as part of the recent Proceedings of the 5th ACM Workshop on Moving Target Defense.

More information: Zhan Shu et al, Ensuring Deception Consistency for FTP Services Hardened against Advanced Persistent Threats, *Proceedings of the 5th ACM Workshop on Moving Target Defense - MTD '18* (2018). DOI: 10.1145/3268966.3268971

Provided by Binghamton University