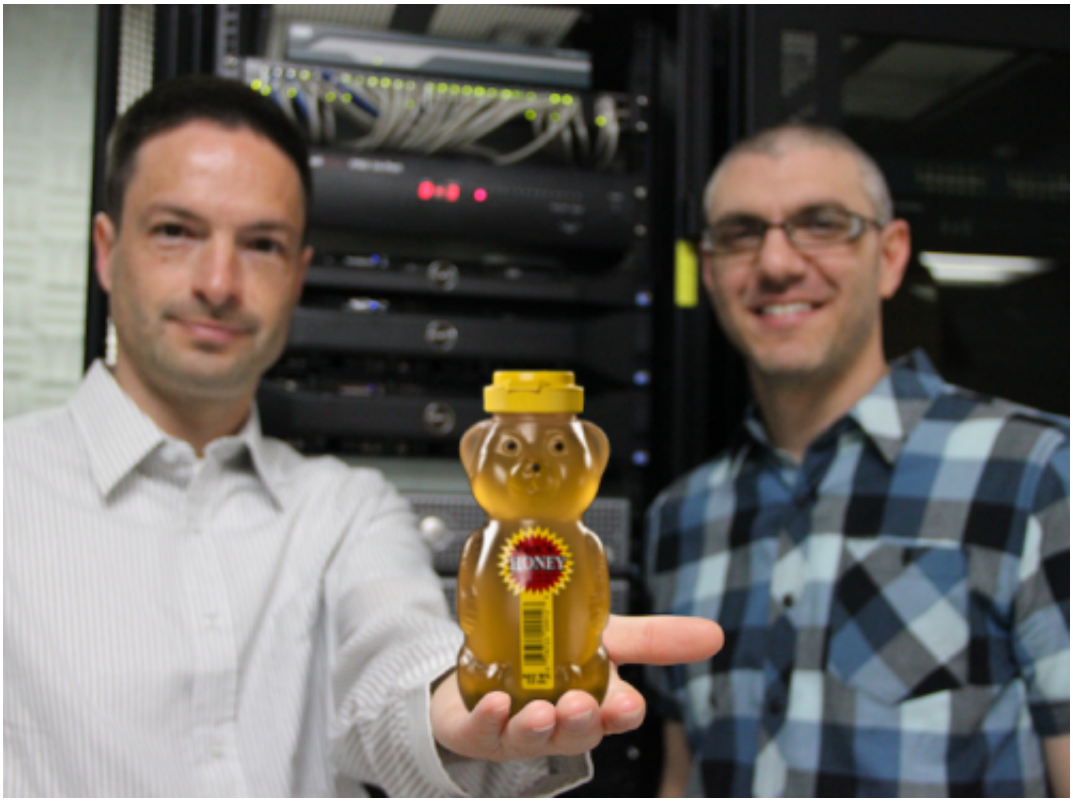
Warning computer hackers shortens their intrusion

January 17 2014, by Andrew Roberts



(Phys.org) —Cybercrime has grown to define the criminal landscape of the 21st century. Yet, cybersecurity research has focused on the crime – computer system attacks – and on counter measures to it, while largely ignoring perpetrator behavior during such attacks. However, University of Maryland researchers now are exploring the conduct of the computer

intruders. In a groundbreaking new study, they show for the first time that the appearance of a warning banner upon entry significantly shortens the time an intruder remains on an attacked system.

The researchers also found that slow network speed combined with a warning message further hastens criminal hackers' departure from the system.

Led by Assistant Professor of Criminology and Criminal Justice David Maimon, the UMD team's research, recently published in the journal Criminology, demonstrates the potential to influence hackers' behavior by targeting their responses to warning messages during attacks. This study is just the "tip of the spear" in criminology-based hacker behavior research and they have additional studies already nearing completion or well underway, according to Maimon.

"There is a lot of literature and research on the effects of deterrents – how to discourage criminal activity," says Maimon. "However there's almost no research on the immediate impact of these efforts, in this case warning messages, on what's happening during the act. In our study we're effectively able to watch a heist in progress, instead of investigating a crime scene after the fact."

Maimon and study colleagues Michel Cukier, associate director for education in UMD's Maryland Cybersecurity Center (MC2) and an associate professor of reliability engineering in Maryland's A. James Clark School of Engineering; Bertrand Sobesto, a Clark School Ph.D. student; and Mariel Alper, a Ph.D. student in the department of Criminology and Criminal Justice, note their research is filling an important void.

A number of industry regulators, such as the National Institute of Standards and Technology (NIST), have developed national guidelines

and policies regarding the display of warning messages when a cyber attack, or intrusion, takes place. However, these policies are largely influenced by the experiences of industry leaders, and are seldom designed around research that supports their effectiveness.

As a result, the UMD team notes, recommendations are being made on a national and global scale, without sufficient testing to prove their value in various environments. These recommendations substantially influence the approach institutions and corporations take to combat cybercrime and if these are misguided, it may have long term implications for the integrity of their security protocols.

The Maryland researchers conducted their study by deploying massive systems of high-interaction "honey pots," or computers that appear to be part of a network, but are actually isolated. These highly monitored systems are designed to study hackers and precisely document their tactics.

By using several hundred "honey pots," altering their system configurations and observing how computer hackers respond, Maimon and his collaborators learned a great deal about the attacks and the attackers. "Think about the burglar analogy. The low-interaction systems, used in a number of other studies, are equivalent to a façade," Maimon explains. "The high-interaction systems we use are like watching criminals break into multi-story homes that are under intense surveillance."

"There's a high percentage of human interaction here," says Maimon. "These aren't 'BotNet' attacks. These are people committing crimes, sitting in front of a computer." By capturing massive amounts of data in these environments, and applying new methods of translated code into behavioral actions, Maimon can literally observe and analyze hackers' keystrokes and draw conclusions about the hackers' tactics and their

reactions to warning messages. "Through extensive collaboration, with the right tools to analyze data on cyber attacks, the application of these newly formed behavioral models can help to mitigate the effects of hacking by applying effective interventions." The findings have tremendous implications for both technology and the social sciences.

Their application of criminological theory to cybercrime is part of a new and a growing field of research into behavior of the individuals who carry out the attacks. "We're combining computers and 'soft science' models for the first time," says Maimon. "We can see that we're making an impact…but there is a great deal left to learn. What kinds of warnings are most effective? Are we able to influence the hackers' behavior over time? These questions will define how our research progresses…and ultimately the future of how we confront cybercrime."

Maimon says he and colleagues are already taking the next steps in applying criminological models to the prevention of computer system trespassing through underway studies that examine:

- how different kinds of warning messages might influence attackers' behavior; and
- how the presence of surveillance mechanisms changes the behavior of computer system trespassers.

More information: Maimon, D., Alper, M., Sobesto, B. And Cukier, M. (2014), "Restrictive Deterrent Effects Of A Warning Banner in an Attacked Computer System." *Criminology*, 52: 33–59. DOI: 10.1111/1745-9125.12028

Provided by University of Maryland

Citation: Warning computer hackers shortens their intrusion (2014, January 17) retrieved 17 April 2024 from https://phys.org/news/2014-01-hackers-shortens-intrusion.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.