START
NATIONAL CONSORTIUM FOR THE
STUDY OF TERRORISM AND RESPONSES TO TERRORISM

RESEARCH BRIEF

A Surveillance Banner on Compromised Computer Systems Reduces Hackers' Active Engagement

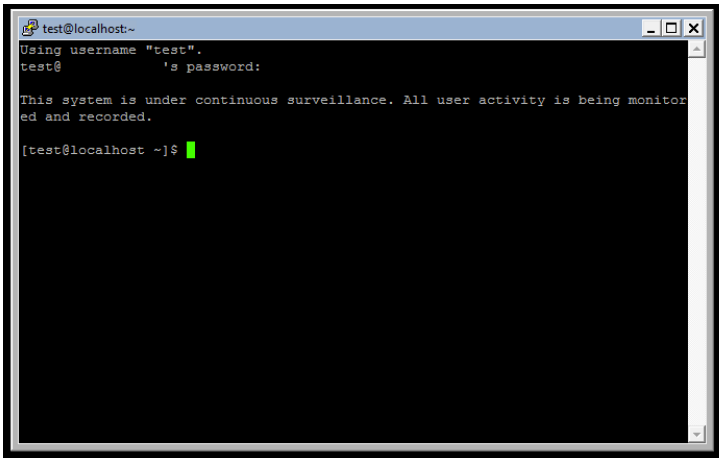
OVERVIEW

This study tested whether the presence of a surveillance message on a compromised computer system would influence a system trespasser's decision to actively engage with the system by entering computer commands.

PROJECT BACKGROUND

This work was guided by deterrence theory toward assessing the effect of a surveillance message in reducing the frequency and severity of hacker behavior on a compromised system. Specifically, the study assesses whether a surveillance message has a restrictive deterrent effect toward hackers limiting the frequency and severity of their system trespassing. This investigation is one of many in a series of projects testing different treatments within randomized controlled trial designs. The primary goal of this work, and the related inquiries, is to discover and evaluate security measures driven by the human component with regard to cybercrime.

METHOD



```
Using username "test".
test@             's password:

This system is under continuous surveillance. All user activity is being monitor
ed and recorded.

[test@localhost ~]$
```

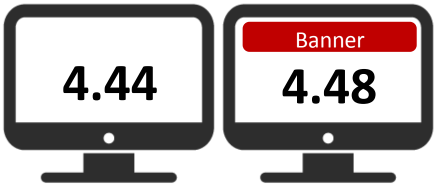
The study originates from a randomized controlled trial conducted at a large public university in the United States. Over a seven-month experimental period, 660 target computer systems were deployed after being compromised by system trespassers. These systems produced 2,942 system trespassing incidents.

Each of these systems was randomly assigned to either display a surveillance banner (n=324) or not display a surveillance banner (n=336) upon each entry to the relevant system.

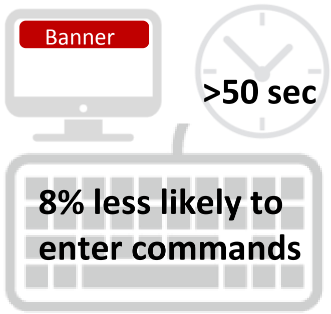
The surveillance banner is depicted at left exactly as the intruders saw it, with the message: "This system is under continuous surveillance. All user activity is being monitored and recorded."

FINDINGS

The surveillance banner did not have an effect upon the frequency of system trespassing incidents on the compromised systems; the average numbers of system trespassing incidents per computers were 4.44 and 4.48 incidents for no surveillance banner and surveillance banner computers, respectively. However, the presence of a banner did affect the seriousness of trespassing incidents.



Trespassing Incidents per Computers



An evaluation of whether computer commands were entered during the first system trespassing incident revealed a consistent pattern with decreased likelihoods of entered commands for hackers that spent more time on the system.

Intruders receiving a surveillance banner that spent at least 50 seconds on the system were 8% less likely to enter commands into the system than respective intruders that did not receive a surveillance banner.

System trespassers who studied the banner for longer periods of time opted to exit the system without entering commands.

A similar restrictive deterrent effect on active engagement with the system was observed for the second trespassing incident, but only for those hackers who had not previously entered commands into the system during the first trespassing incident.

Of those that did not previously enter commands into the system, 38% of those with the surveillance banner and 47% of those with no surveillance banner entered commands during the second trespassing incident. This difference was found to be statistically significant.

Those who entered commands during the first trespassing event were far more likely to enter additional commands than those who did not during the first session.

Of those that did previously enter commands into the system, 67% of those with the surveillance banner and 63% of those with no surveillance banner entered commands during the second trespassing incident.

IMPLICATIONS

An intruder cannot damage or pilfer a system without entering computer commands into that system. While the employed surveillance banner did not reduce the total number of trespassing incidents, it did affect the likelihood of an intruder escalating their offending by typing into the system on the first and second trespassing incidents. These findings offer modest support for the application of restrictive deterrence in the study of system trespassing.

FUTURE DIRECTIONS

Future research should employ and test both stronger messages as well as more active forms of surveillance on compromised systems.

RESEARCHERS AND CONTACT INFORMATION

Project Lead: Theodore Wilson
Other Project Researchers: David Maimon, Bertrand Sobesto, and Michel Cukier

To provide feedback, or for any correspondence relating to this research, or for a copy of the full report on this topic, please contact:

Theodore Wilson
Doctoral Student
Department of Criminology and Criminal Justice
University of Maryland
2158 LeFrak Hall
(301) 405-8092; twilson5@umd.edu

This research brief is based on an article in the Journal of Research in Crime and Delinquency, “The Effect of a Surveillance Banner in an Attacked Computer System Additional Evidence for the Relevance of Restrictive Deterrence in Cyberspace.”

START

The National Consortium for the Study of Terrorism and Responses to Terrorism (START) is supported in part by the Science and Technology Directorate of the U.S. Department of Homeland Security through a Center of Excellence program based at the University of Maryland. START uses state-of-the-art theories, methods and data from the social and behavioral sciences to improve understanding of the origins, dynamics and social and psychological impacts of terrorism. For more information, contact START at infostart@start.umd.edu or visit www.start.umd.edu.

This research was supported by the National Science Foundation through awards made to the START and the authors. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the National Science Foundation or START.