JOURNAL WATCH

Mobile Malware Mutates

A new study analyzing more than a million samples of Android malware illustrates how malicious apps have evolved over time. The results, published in *IEEE Transactions on Dependable and Secure Computing*, show that malware coding is becoming more cleverly hidden, or obfuscated.

Malware in Android phones is "still a huge issue" says Guillermo Suarez-Tangil, a researcher at King's College London who co-led the study. "A central challenge is dealing with malware that is repackaged."

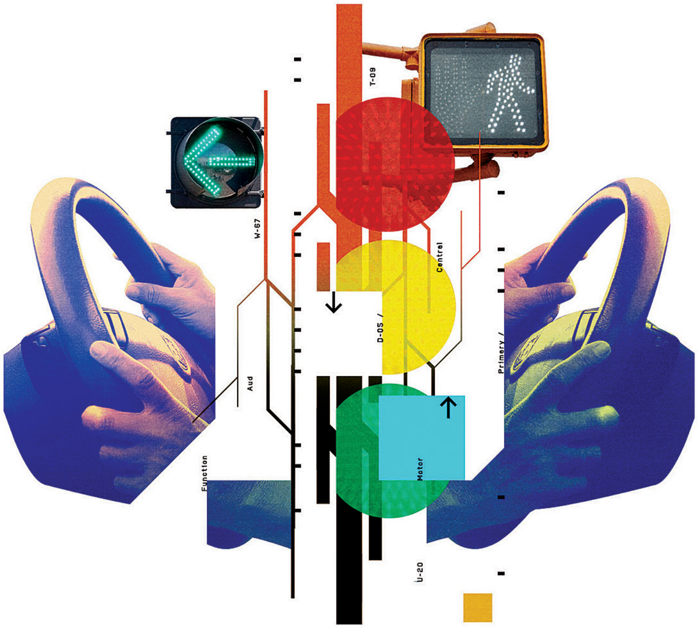
Repackaged malware contains malicious coding that's embedded within legitimate apps. Suarez-Tangil and his coauthor, Gianluca Stringhini of Boston University, developed a technique involving differential analysis to slice the malicious coding from the benign parts and study the behavior of the malicious slice. They applied it to 1.2 million samples of malware circulated between 2010 and 2017.

Suarez-Tangil and Stringhini found there has been a major shift away from malware that supports premium rate fraud, whereby expensive SMS messages are sent to users. While this type of coding was seen in 40 percent of malware families in 2013, its prevalence dropped to 10 percent in late 2016.

One feature that's on the rise is the amount of malware that's obfuscated. "In particular, we observed that cryptography is present in 90 percent of the recent families [of malware]," says Suarez-Tangil. "To the best of our knowledge, there are only a few malware-detection systems capable of dealing with these forms of obfuscation, and they all have limitations."

Overall, this study shows that malware is evolving to be more sophisticated—and sneaky. Suarez-Tangil says researchers will need to rely on techniques such as machine learning and dynamic program analysis to keep pace. **—MICHELLE HAMPSON**

An extended version of this article appears on our website in the Journal Watch section.



nizers will begin recruiting drivers and installing onboard units in July, with testing to begin in November.

The technology will enable "basic safety messaging," including warnings to reduce speed or look out for pedestrians ahead, explains Luke Stedke, who manages communications at Drive Ohio, the state's smart-mobility center. The pilot is part of the Smart Columbus initiative, which was launched after the city won US $40 million in the U.S. Department of Transportation (DOT)'s 2015 Smart City Challenge.

Columbus joins two other cities in Ohio–Marysville and Dublin–that have recently begun testing connected vehicles. Collectively, the DOT has invested more than $45 million in such trials in Wyoming, Tampa, and New York City.

The keen interest in connecting nonautonomous vehicles comes primarily from the technology's potential to reduce crashes and save lives, says Debra Bezzina, of the University of Michigan's Transportation Research Institute. Sensors to alert drivers to hazards in their blind spots, streetlight-mounted cameras that show a pedestrian at an upcoming intersection, and an approaching car that warns of black ice ahead are just a few examples of what may be possible.

"Connected-vehicle technology can prevent 80 percent of all unimpaired car crashes," says Bezzina. "So it could save billions of dollars a year."

The new technology also promises more efficient traffic management and greener commuting. Emergency vehicles could move through intersections quicker with all the lights in their favor. Motorists, using information broadcast by traffic signals about their phase and timing, could adjust their speed accordingly and save fuel.

Connected-vehicle communications can run either on a wireless technology called Dedicated Short-Range Communications (DSRC) or on a cellular-based

ILLUSTRATION BY Stuart Bradford