NYU TANDON SCHOOL OF ENGINEERING
11201

PRESS OFFICE • 1 MetroTech Center, 19th Floor, Brooklyn, NY

CONTACT • Karl Greenberg
646.997.3802 / mobile 646.519.1996
Karl.Greenberg@nyu.edu

Immediate Release

Tandon team shines light on roiling market for stolen debit and credit cards

NYU Tandon researcher Damon McCoy analyzed a database containing more than 26 million credit and debit card records, discovering that even cards with anti-counterfeiting chips are vulnerable because consumers still use the hackable magnetic stripe

BROOKLYN, New York, Monday, August 3, 2020 – Much of the world has switched to embedded anti-counterfeit EMV (Europay, MasterCard, Visa) chips in credit cards, but adoption in the U.S. lags. Therefore, a significant percentage of the U.S. population is vulnerable to theft by "skimming" and other means of stealing data from magnetic stripes during the transactional process, which is then used to produce counterfeit cards or to monetize data through other illicit activities.

Damon McCoy, assistant professor of computer science and engineering at the NYU Tandon School of Engineering, and a team of Tandon colleagues analyzed data from 2015 to 2019 that had been extracted from BriansClub, an underground bazaar for buying stolen and leaked credit card information.

The study, "Swiped: Analyzing Ground-truth Data of a Marketplace for Stolen Debit and Credit Cards," the first inside analysis of an underground marketplace for stolen credit and debit cards, found that chip-enabled cards are no guarantee of security if owners still swipe the stripe: the investigators found that in the last two years of the leaked data, **85% of the stolen magnetic stripe data originated from EMV chip-enabled cards**.

"Current incentives might be insufficient to reduce risky use and acceptance of magnetic stripe transactions," said McCoy. "And even three years after the liability shift to EMV chips, there still was a small but persistent supply of newly issued cards without chips, especially among prepaid cards." He said that such non-EMV accounts saw much greater demand than EMV accounts and made up 30.4% of the illicit shop's gross revenue after the liability shift.

-more-

The database was filched from BriansClub in 2019 by a white-hat hacker who extracted more than 26 million credit and debit card records that thieves had stolen from online and brick-and-mortar stores. These were supplied to the publication Krebs on Security. The security news and investigative journalism site then shared the database with McCoy, among others.

The team, including Tobias Lauinger, a postdoctoral researcher; and Maxwell Aliapoulios, Rasika Bhalerao, and Cameron Ballard, Ph.D. candidates under McCoy's direction, analyzed the leaked transactional data to characterize BriansClub's business model, sellers, customers, and finances. Between 2015 and 2019 the shop earned close to $104 million in gross revenue and listed more than 19 million unique card numbers for sale. They found that while 97% of the inventory was obtained from magnetic stripes taken during in-person transactions, customers purchased only 40% of this inventory. By contrast, BriansClub sold 83% of its card-not-present inventory, used for online fraud, which appeared to be in short supply. Demand and pricing were not uniform, as buyers appeared to perceive some banks as having weaker countermeasures against fraud.

Additionally, out of the more than 19 million accounts listed in the shop, 60% did not find buyers, despite prices starting at only 21 cents.

“We investigated what made such a large fraction of stolen accounts apparently undesirable for malefactors and found that they preferred to purchase magnetic stripe accounts issued by certain banks but not others,” said McCoy. “In particular, thieves appeared to prefer accounts from medium-sized and smaller banks.”

Among the findings were:

- The rise in chip-cards has driven an increase in e-merchant / card-not-present fraud
- Only 27% of American Express card data was purchased; the smallest number from a large institution
- Cards issued in specific states — like South Carolina — were more likely to have their data purchased
- USAA, a savings bank with fewer regional locks, was a significant target
- BriansClub made $24 million in profit selling stolen credit card information over just four years

The research was supported by a grant from the National Science Foundation.

About the New York University Tandon School of Engineering

The NYU Tandon School of Engineering dates to 1854, the founding date for both the New York University School of Civil Engineering and Architecture and the Brooklyn Collegiate and Polytechnic Institute. A January 2014 merger created a comprehensive school of education and research in engineering and applied sciences as part of a global university, with close connections to engineering programs at NYU Abu Dhabi and NYU Shanghai. NYU Tandon is rooted in a vibrant tradition of entrepreneurship, intellectual curiosity, and innovative solutions to humanity’s most pressing global challenges. Research at Tandon focuses on vital intersections between communications/IT, cybersecurity, and data science/AI/robotics systems and tools and critical areas of society that they influence, including emerging media, health, sustainability, and urban living. We believe diversity is

integral to excellence, and are creating a vibrant, inclusive, and equitable environment for all of our students, faculty and staff. For more information, visit engineering.nyu.edu.

###

www.facebook.com/nyutandon

@NYUTandon