MOTHERBOARD
TECH BY VICE

Hacker Who Stole $5 Million By SIM Swapping Gets 10 Years in Prison

A 20-year-old college student who was accused of stealing more than $5 million in cryptocurrency in a slew of SIM hijacking attacks is the first person to be sentenced for the crime.

By **Lorenzo Franceschi-Bicchierai**

Feb 2 2019, 3:19am

IMAGE: LORENZO FRANCESCHI-BICCHIERAI

A college student who stole more than $5 million in cryptocurrency by hijacking the phone numbers of around 40 victims pleaded guilty and accepted a plea deal of 10 years in prison, Motherboard has learned.

Joel Ortiz accepted the plea deal last week, Erin West, the Deputy District Attorney in Santa Clara County, California, told Motherboard during a meeting on Thursday. The authorities believe Ortiz is the first person to be convicted of a crime for SIM swapping, an increasingly popular and damaging hack. The prosecutors and agents who have been investigating these hacks celebrated the conviction, and said they hope that this will serve as an example for the other alleged criminals who have already been arrested, as well as the ones who have yet to be caught.

"We think justice has been served. And hopefully this is a strong message to that community," Samy Tarazi, one of the agents who investigated the Ortiz case, told me.

> *Got a tip? You can contact this reporter securely on Signal at +1 917 257 1382, OTR chat at lorenzofb@jabber.ccc.de, or email lorenzofb@vice.com*

Ortiz is one of a handful of SIM swappers who have been arrested in the last year for hijacking phone numbers and using them to then hack into emails, social media accounts, and online Bitcoin wallets. Other people who have been arrested are Xzavyer Narvaez, who's accused of stealing around $1 million in Bitcoin; Nicholas Truglia, who's also accused of stealing millions in Bitcoin; and Joseph Harris, one of the most infamous SIM swappers who allegedly stole more than $14 million in cryptocurrency.

The authorities think the slow but constant drip of arrests, and Ortiz's sentencing, will send a clear message to those who are still out there.

"Each arrest that we made sent shockwaves through that community," West said. "That they weren't safe in their basement, they weren't safe in their room in their mom's house, that they were being tracked down and arrested—one by one."

West added that "in looking at Joel's sentence—10 years—it shows that our community will not tolerate this type of crime. And we will continue to find everyone who's responsible."

> *Read more: How To Protect Yourself From SIM Swapping Hacks*

West and her colleagues declined to say how many ongoing investigations they have, but she said that they have made new arrests and served new search warrants.

Almost all these investigations have stemmed from the Regional Enforcement Allied Computer Team or REACT, a task force of multiple local California police departments. Tarazi, an agent at REACT, said that during 2018, they received hundreds of reports of SIM swapping attacks from victims. Those reports, according to him, have now slowed down.

Ortiz will be officially sentenced on March 14.

Listen to CYBER, Motherboard's new weekly podcast about hacking and cybersecurity.

TAGGED: TECH, MOTHERBOARD, NEWS, CYBERSECURITY, INFOSEC, CYBERCRIME, TECH NEWS, SIM CARDS, REACT, SIM SWAPPING, SIM HIJACKING, PORT OUT SCAM, JOEL ORTIZ

Watch This Next

How a Hacker Convinced Motorola to Send Him Source Code

FROM **GREATEST MOMENTS IN HACKING HISTORY**

MOTHERBOARD
TECH BY VICE

AT&T Contractors and a Verizon Employee Charged With Helping SIM Swapping Criminal Ring

The indictments show that sometimes stealing phone numbers to hack accounts is an inside job.

By **Lorenzo Franceschi-Bicchierai**

May 14 2019, 2:02am

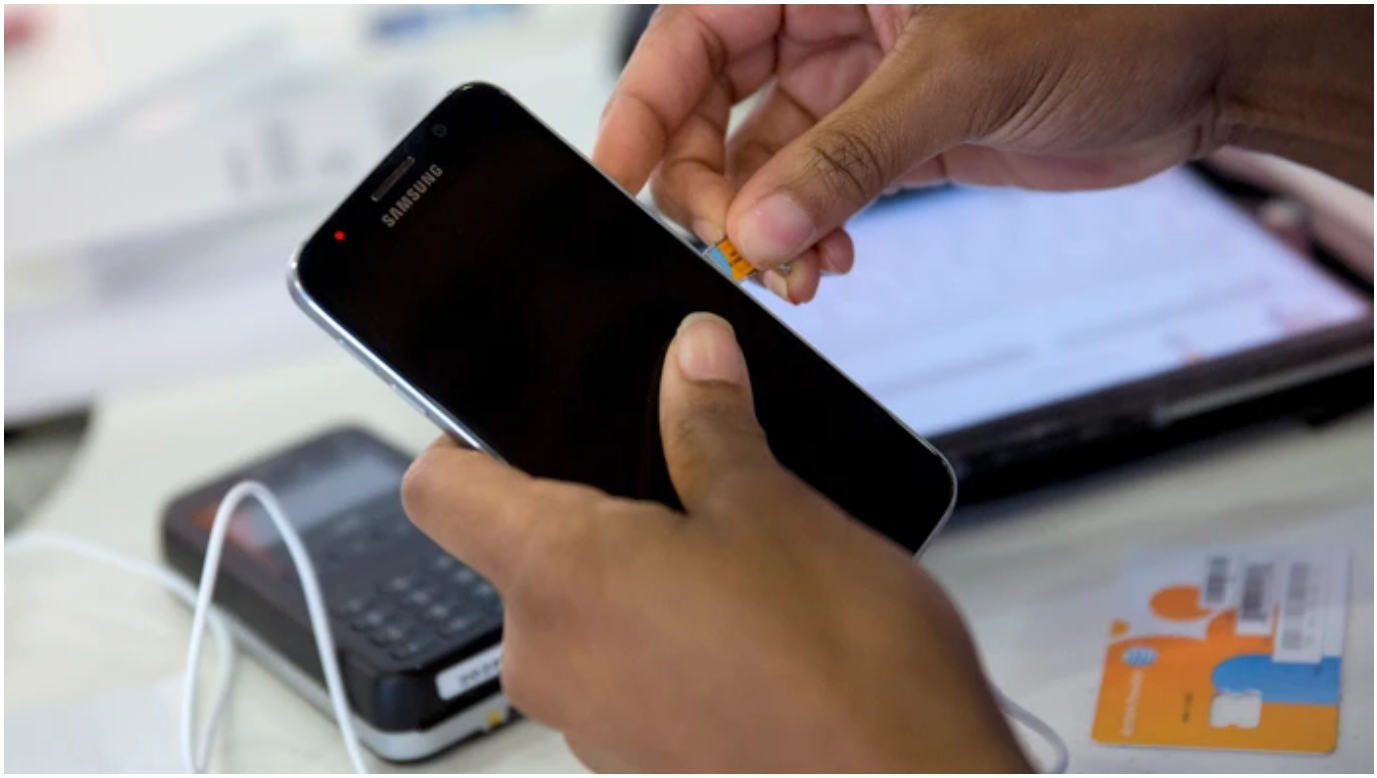

IMAGE: ANDREW HARRER/BLOOMBERG VIA GETTY IMAGES

Last week, the Department of Justice accused nine people of allegedly being part of a crime gang known as "The Community" that hijacked mobile phone numbers to then steal money and cryptocurrency. This is yet another criminal case brought forward against hackers who use a technique called SIM swapping to target bank accounts and, primarily, online cryptocurrency wallets.

Among the alleged criminals were also two former AT&T contract employees and one former Verizon employee, who helped the alleged criminals by providing private customer information in exchange for bribes, according to court documents.

SIM swapping, sometimes referred to as SIM hijacking or port out scam, if a type of fraud where criminals take over victim's phone numbers and then use them to steal money. SIM swapping is a popular technique among criminals because it can bypass traditional security mechanisms such as two-factor authentication. Criminals either trick telecom employees into giving them control of the victim's phone numbers, or bribe them in exchange for their help. Telecom employees can perform SIM swaps as part of their jobs (say, if the customer has lost their phone) or can provide personal information that helps the criminals impersonate the victim.

The two former AT&T contractors in Tucson, Arizona were Robert Jack and Jarratt White.

> *Have a tip about a SIM swapping case? You can contact this reporter securely on Signal at +1 917 257 1382, OTR chat at lorenzofb@jabber.ccc.de, or email lorenzo@motherboard.tv*

White allegedly received bribes from one of the criminals who was part of "The Community," according to a criminal complaint. White, according to the feds, helped the criminals steal more than $2 million from several victims by performing 29 fraudulent SIM swaps. White communicated with the criminals via Telegram, according to the document.

Jack, who was an associate of White, allegedly performed twelve fraudulent SIM swaps in May of 2018. White allegedly paid Jack $585.25 for his help in the SIM swapping conspiracy, according to the complaint.

An AT&T spokesperson said in an email that this case "involves two former vendor employees that we reported to law enforcement."

Fendley Joseph used to work for Verizon in Murrieta, California, according to the criminal complaint and his LinkedIn profile.

He is also accused of accepting bribes in exchange for helping The Community's criminal SIM swapping activities. With Joseph's help, the criminals allegedly stole $100,000, according to the complaint.

Joseph did not perform SIM swaps himself. Instead, he would give the criminals private information about the targets, which would help them impersonate the victim and take over their phone number. Joseph allegedly earned $3,500 from one of the criminals, according to the court document.

A Verizon spokesperson confirmed that Joseph was once an employee, but declined to comment any further.

White, Jack, and Joseph are the first telecom employees to be indicted in a SIM swapping case. But they may not be the last ones. As Motherboard reported last year, criminals involved in SIM swap fraud often recruited employees who work at cellphone carriers.

"Everyone uses them," someone who claimed to be a SIM hijacker told Motherboard last year. "When you tell someone they can make money, they do it."

One T-Mobile employee who spoke to Motherboard at the time said the criminals found him via Instagram, and then offered him $100 per target.

Robert Ross, a tech entrepreneur who launched a website to support victims of SIM swapping and pressure telcos to protect their customers, said these indictments prove the companies could have done better.

"This isn't social engineering anymore," Ross, who was SIM swapped last year, said in an online chat. "The story needs to move from 'the carriers aren't doing enough to fix the problem' to 'the carriers have no control over their tens of thousands of customer service reps and knowingly allowed them to be bribed."

Listen to CYBER, Motherboard's new weekly podcast about hacking and cybersecurity.

Correction: The original headline for this story was "AT&T and Verizon Employees Charged With Helping SIM Swapping Criminal Ring." We have updated the headline to clarify that Robert Jack and Jarratt White weren't employed by AT&T directly, but by another company that was contracted by AT&T.

This story has been updated to include comments from AT&T and Verizon spokespeople.

TAGGED: SECURITY, INFOSEC, CYBERCRIME, VERIZON, AT&T, INFORMATION SECURITY, SIM SWAPPING, SIM HIJACKING, PORT OUT SCAM

Watch This Next

How a Hacker Convinced Motorola to Send Him Source Code

FROM **GREATEST MOMENTS IN HACKING HISTORY**