Nigerian hacker pleads guilty to stealing payroll deposits

By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)** February 23, 2022 01:47 PM **1**

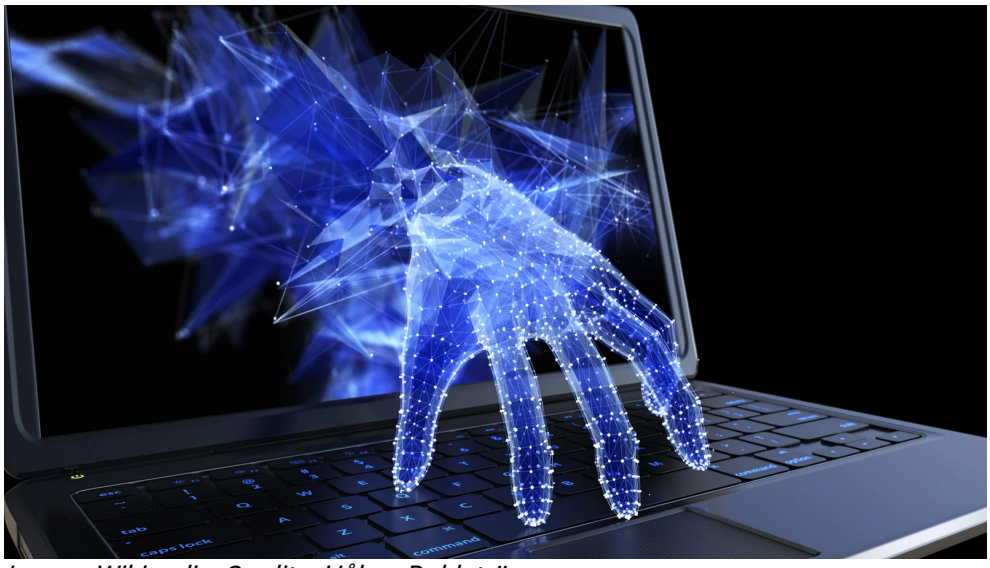


Image: Wikipedia, Credits: Håkan Dahlström (https://www.flickr.com/people/93755244@N00)

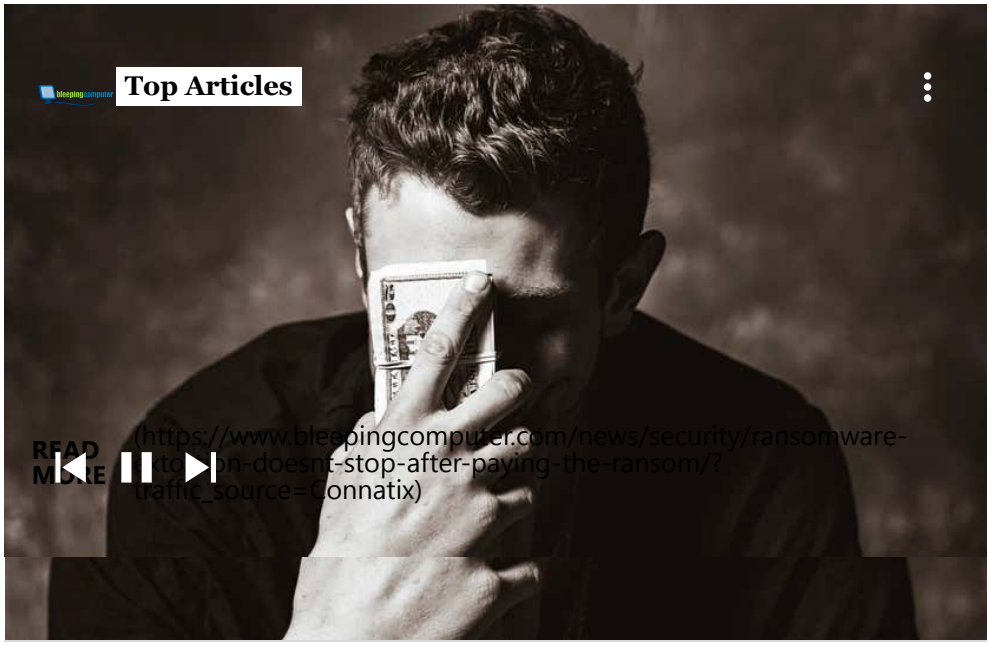
A Nigerian national named Charles Onus has pled guilty in the District Court of the Southern District of New York to hacking into a payroll company's user accounts and stealing payroll deposits.

According to the indictment and the statements made in court, Onus was actively involved in a scheme that took over user accounts of company employees across the United States and stole payroll deposits by diverting the salary payments to debit cards under his control.

This malicious activity started in July 2017, and until the time of his arrest, Onus had compromised 5,500 user accounts to divert a total of $800,000 in payroll funds.

Exploiting a hole in account security

The threat actor used credential stuffing (https://www.bleepingcomputer.com/news/security/ripe-ncc-internet-registry-discloses-sso-credential-stuffing-attack/) attacks to gain access to accounts at a human resources and payroll company responsible for making salary payments for other company's employees.



Credential stuffing is a type of cyberattack where threat actors use username and password combinations taken from previous data breaches and attempt to use those credentials to log in at other online sites.

The method is different from brute-forcing or guessing the passwords, as it doesn't involve cracking but instead relies on the victim reusing the same credentials on multiple platforms.

"After a Company user account was compromised, the bank account information designated by the user of the account was changed so that Onus would receive the user's payroll to a prepaid debit card that was under Onus' control," details the DOJ announcement (https://www.justice.gov/usao-sdny/pr/nigerian-national-pleads-guilty-participating-scheme-conduct-cyber-intrusions-steal).

The arrest of Charles Onus came on April 14, 2021, when the defendant flew from Abuja, Nigeria, to San Francisco, where he was arrested at the airport.

The defendant has now pled guilty to one count of computer fraud for accessing foreign computer networks without authorization. This carries a maximum sentence of five years in prison, and the actual punishment is to be decided by Judge Gardephe on May 12, 2022.

Defending against credential stuffing

A simple way to thwart credential stuffing attacks is to use some form of multi-factor authentication (MFA), which requires a separate authorization code in addition to a user name and password.

As these codes are usually sent to a user via SMS text or using an authentication app, even if a threat actor has a stolen login name and password, they would not be able to log in without the MFA one-time passcode.

Online platforms may also employ fingerprint-based anti-stuffing systems to detect these automated login attempts and block repeated attempts. However, if the number of login attempts is small, it's not easy to filter them out.

These attacks are the reason why password recycling is a bad idea and why users should globally reset their passwords once they've been compromised on any site.

Furthermore, users should utilize a password manager and unique passwords at every site they have an account to prevent a data breach at one site, affecting their accounts at other sites.