Back to School: BEC Group Targets Teachers with Payroll Diversion Attacks

intelligence.abnormalsecurity.com/blog/bec-group-targets-teachers-payroll-diversion-attacks

Discover how threat group Chiffon Herring leverages impersonation and spoofed email addresses to divert paychecks to mule accounts.

Fall in the northern hemisphere is marked by a variety of things: leaves changing colors, the sun setting earlier, and the ubiquitous return of pumpkin spice flavoring. For many parents and their children, it's also time to go back to school—whether they're ready for summer to be over or not.

Unfortunately, some scammers exploit the back-to-school season for their own nefarious purposes. Like most financially-motivated cybercrime, business email compromise (BEC) attacks are generally industry agnostic, meaning attackers don't specifically target certain industries or companies. Rather, financially-motivated cybercriminals try to maximize their return on investment by casting a wide net of potential victims.

However, our Abnormal team has identified a specific group bucking this trend, which we call Chiffon Herring. The group has been active since at least March 2022 and mainly targets local school districts and universities in the United States.

Their targets have ranged from large public universities to small community colleges, and from sprawling urban school districts to an individual all-girls preparatory school. Based on our research, Chiffon Herring actors are likely located in Nigeria and South Africa, both of which are typical hotbeds for BEC scammers.

A Background on Payroll Diversion

Payroll diversion is a popular form of business email compromise where an attacker targets a human resources administrator and impersonates an employee (usually an executive) to request a change to the employee's direct deposit account information.

In its early days, payroll diversion attacks almost exclusively targeted organizations in the United States. But in recent years, these attacks have shifted and are now targeting employees across the world—specifically in Western Europe and Australia.

The payroll diversion landscape is primarily driven by the use of mule accounts, or accounts that receive fraudulent funds, at non-traditional financial technology institutions. Accounts linked to prepaid cards or third-party apps like Green Dot or CashApp make up an overwhelming percentage of the mule accounts associated with payroll diversion attacks.

Setting the Hook: A Look at Chiffon Herring's Emails

Chiffon Herring is notably unique in that the group almost exclusively targets local school districts and universities.

The general structure of an attack from this group is similar to many other payroll diversion attacks. However, instead of impersonating company executives, Chiffon Herring generally poses as non-executive employees like teachers and professors and sends the attacks to the department head at a university or office staff at a school district. Because their names and email addresses are publicly listed on most school websites, these individuals can be incredibly easy to impersonate and target.

An initial email from Chiffon Herring indicates the impersonated teacher has recently changed banks and needs to update their direct deposit information. The email also mentions that the previous account will be inactive a few days before the next payday, injecting some urgency into the request.

Example of an initial Chiffon Herring email

A notable tactic used by Chiffon Herring is spoofing the email address of the teachers they impersonate, which makes the email seem as if it's coming from a teacher's legitimate email account. Behind the scenes, however, the reply-to address is a Gmail or mail.com account controlled by the attacker, which is where any subsequent communications would be sent.

Schools can often be an easier target for attackers because they are unlikely to have stringent cybersecurity protocols—unlike large enterprises or government entities. In the case of the institutions targeted here, there is either no published DMARC record in place or it is not configured to reject unauthorized senders. This allows the attackers to use the exact domain and thus bypass legacy systems that check only for this header information to detect attacks.

In addition to spoofing impersonated teacher email addresses, an analysis of email headers reveals Chiffon Herring also leverages GoDaddy infrastructure to send the attacks. The “Workspace Webmail 6.12.10” user agent string referenced in the headers indicates the emails are coming from GoDaddy’s webmail service, and the domains referenced in the header “return-path” field signals a potentially compromised domain. The abuse of GoDaddy domains to send malicious email campaigns is a longstanding problem that has been around for years.

Header analysis of a Chiffon Herring email

Reeling It In: Where the Stolen Teacher Paychecks Go

If a targeted employee responds to the initial email from Chiffon Herring, the attack moves into the second stage. In this stage, the attacker provides details for a mule account to which they want the impersonated teacher’s paycheck diverted.

Our team conducts active defense engagements with BEC actors to better understand the full cycle of BEC attacks, including identifying mule accounts scammers use to receive fraudulent funds. In this case, we were able to identify one of the accounts associated with this group.

Chiffon Herring email containing mule account information

Chiffon Herring almost exclusively provides Green Dot accounts as an initial “replacement” direct deposit account, which are generally linked to prepaid cards. Prepaid cards are commonly used in payroll diversion attacks because many card issuers offer the option to receive direct deposits up to 48 hours before a payday. This means that the threat actors have access to the diverted funds for multiple days before the teacher even realizes anything is wrong.

The accounts are also relatively easy to open. A prepaid card can be obtained at a big box store like Walmart, and then once the card is “registered,” a checking account is created that can be used to receive funds. An account can also be opened online using a fake identity and the new account details are emailed to a scammer.

Securing Schools Against Cybercrime

Threat actors continue to execute these attacks because they work. They have spent years perfecting the writing of these emails to make them look as legitimate as possible. And because they are not often the target of coordinated cyberattacks, many schools may not be aware that they are being targeted by these scams.

To ensure protection against payroll diversion attacks, it is critical that all staff (and particularly those in finance and human resources) are trained to detect the signs of phishing attacks. They should be reminded to read through emails carefully, and pay close attention to the email addresses to make sure they are actually coming from the sender—especially when discussing something related to finances.

It’s also important to implement an email security solution that can detect signs of attacks and block malicious emails before they reach their intended recipient. Innovative solutions use behavioral AI to analyze identity and content and then separate legitimate messages from dangerous threats. By baselining known-good behavior and detecting anomalies, modern email security solutions can block the socially-engineered attacks that bypass legacy systems.

See how Abnormal protects educational organizations from the full spectrum of attacks. Request a demo today.

Appendix: Observed Email Addresses Linked to Chiffon Herring BEC Attacks

adleymarcc565[@]gmail[.]com
bankroll630[@]gmail[.]com
barbara.hiring[@]gmail[.]com
briannanicholas81[@]gmail[.]com
caseybrown847[@]gmail[.]com
deloreschapman6[@]gmail[.]com
directtdepositoffice00[@]email[.]com
gatekelvin2229[@]gmail[.]com

ginalocker9[@]gmail[.]com
godchoice088[@]gmail[.]com
gtaylor9833[@]gmail[.]com
hellen.brown18[@]yahoo[.]com
jilllain777[@]gmail[.]com
johnrazoo820[@]gmail[.]com
kathygros1313[@]gmail[.]com
larryeppler8[@]gmail[.]com
laurastiles1010[@]gmail[.]com
laureljames750[@]gmail[.]com
luigi.cuneo45[@]gmail[.]com
mariastewart314[@]gmail[.]com
mathgradee[@]gmail[.]com
meetfish59[@]gmail[.]com
michealfought21[@]gmail[.]com
msadwick1[@]gmail[.]com
mydirecttdeposittofffice[@]mail[.]com
officeink[@]mail[.]com

payrollnetwork20[@]gmail[.]com

randal200lo[@]gmail[.]com

replydirectmail[@]gmail[.]com

roselynnbrandon[@]gmail[.]com

sadwicksandra[@]gmail[.]com

shelbybilby2[@]gmail[.]com

smithanderson027[@]gmail[.]com

sodibambam[@]yahoo[.]com

steverosewoodautomotive[@]gmail[.]com

sureska57[@]mail[.]com

tj602432[@]gmail[.]com

traymond231[@]gmail[.]com

wdoris938[@]gmail[.]com

whelane28[@]gmail[.]com

williamssamuel1232[@]gmail[.]com

williamssarah3213[@]gmail[.]com