A Study on Mule Fraud and Defense Techniques: School Infrastructure

Quentin Jean Marie Grau
Forensic and Cyber Security Research Centre
Asia Pacific University of Technology and innovation (APU)
Kuala Lumpur, Malaysia
quentin.grau7@gmail.com

Nor Azlina Abd Rahman
Forensic and Cyber Security Research Centre
Asia Pacific University of Technology and innovation (APU)
Kuala Lumpur, Malaysia
nor_azlina@apu.edu.my

***Abstract*— Cybercrimes are numerous and lead to very bad consequences. This paper will focus on Fraud-as-a-Service and more specifically on one of its key components: the mule. The school infrastructure will be discussed as well as its current defense against mule fraud. Its vulnerabilities will be discussed and will see how to counteract them. Finally, will see the general, operational, and technical aspects of the security to be implemented in order to stay protected against this kind of attacks.**

Keywords*— *Cybercrime, cyber defenses, cybersecurity, fraud, mule fraud

I. INTRODUCTION

According to (Rivera et al., 2020), 47% of the respondents said that they had an incident of fraud or economic crime in the last 24 months. Moreover, the total financial impact of the frauds they experienced exceeds $42 billion. Unfortunately, the financial impact is not the only impact towards these organizations, there is also the loss of reputation and/or their market share. Fraud as a Service (FaaS) is a business model used by cyber criminals in order to sell services, or tools, which will be used to commit digital crimes. It involved a network of criminals that work together to run this illegal business, an online platform, often on the dark web, which will host the sale of the criminal services, or tools. The platform can be used to sell hacking services, such as renting a botnet to perform a DDoS attack, buying a ransomware in order to extort victims and earn money, or any hacking service that can be done by a professional hacker for the buyer. Most of the time, the customers of this platform are not qualified in computer science, and just want to earn money with tools such as ransomware or want to damage a company or a person by paying a hacker to get sensitive information about the victim or ruining his/her life.

A key component of this business model is the mule. Indeed, the mule is the person, or organization, that will be used to launder the money. Cyber criminals who may have stolen money or earned it illegally cannot simply deposit it in their bank. The transaction has to be clean for them to get legal money. To do that, they will use the mule and send him money, often by cheque, and ask him/her to send it to another account. The transaction, which come from a clean account (the mule's account), will then be considered as legal. The criminals' money is now laundered(Schifferle, 2020). This scam may happen several ways, it can be because of online dating, where the scammer asks the victim to receive money to send it to another account, it can also be the promise of a work-at-home job that will make the victim earn a lot of money. When the victim is an organization, it will probably come from a cyber-attack that will allows the attacker to change the recipient of a money transfer from the original to a mule account that will receive the money and send it back to another account. They use a mule account since the mule has a clean account from a high-rate bank, while the attackers may not have a reliable bank account, and don't want the police to trace it back to them.

Being a mule is a crime and carries very bad consequences to the person, even without knowing it. Indeed, (Money Mule Awareness, 2019) states that the mule faces prosecution and incarceration of up to 30 years imprisonment and $1 million fine, but his/her personal information may also be compromised because he/she gave it to the criminals before participating in their illegal activities. He/she may have to pack back the money to the victims. This can also have negative consequences on the mule's bank score, he/she may be blocked by his/her bank and may not be able to open any more bank accounts again.

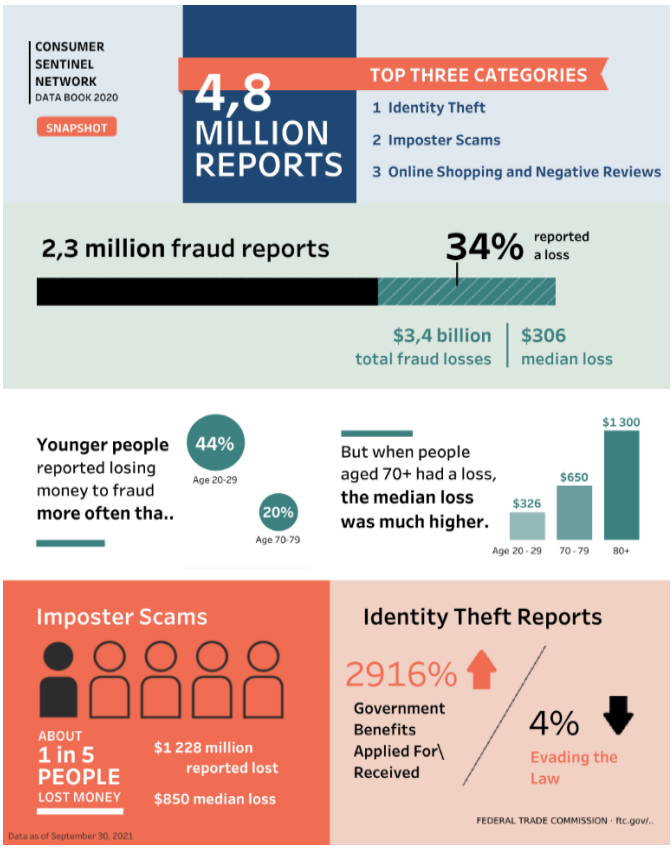

Fig. 1. (Commission, 2021) Data Book 2020

As can see on the diagram above, among the 4.8 million identity theft and fraud reports, 2.3 million are fraud reports. That means that Fraud-as-a-Service is a significant subject within Cybercrime-as-a-Service. This report includes only individual cases. This is why the number of reports is lower than the number of corporate fraud crimes, as attackers prefer to go after companies because of the greater money gain.

This paper will focus on the school infrastructure since the education industry has really suffered from the Covid-19 pandemic. Indeed, it was one of the most unprepared sector against cyber threats. Based on (Cybersecurity, 2020), in July and August 2020, 57% of the ransomware incidents involved school districts. This number doubles at the beginning of the school year, as it is only 28% for the rest of the year. A case study will be discussed about mule fraud towards the school infrastructure in order to get an idea about how this kind of attacks happen against this infrastructure.

II. STUDY ON FRAUD CASES

The first case that we will discuss is the case of a small Texas school district which lost $2 billion because of a Business Email Compromise (BEC) attack(FBI, 2020) [6]. Indeed, the district has been attacked and a mule played a very important role in this attack. A Florida man received the money on his account and transfers it to the overseas accounts of the attackers. The initial attack vector is a fraud email that consisted in a request of transfer for a school construction project. In fact, the school district was planning to build a new school, so the mail didn't seem that strange. The district proceeded to the payment and sent the money directly to the mule account that was controlled by the attackers. The Florida man has been identified because the school noticed that they have been extorted. They contacted law enforcement and an investigation has been conducted. Investigators traced it back to him. He has been arrested and sentenced to almost six years imprisonment. $600,000 has been found in the mule's account, they will surely be returned to the school district's account. A luxury car of the mule has also been seized by law enforcement which has been bought with the money earned thanks to his illegal activities.

Another case is the case of a Miami man that has been sentenced to 5 years in prison after being part of criminal network by playing the role of a mule, and the role of recruiter of 15 other mules (U.S. Attorney's Office, 2013). The attackers have used business email compromise (BEC) and other cyber-schemes in order to extort their victims. The man that played the role of the money mule has also been sentenced to 3 years of supervised release and had to pay more than $700,000 fine to restitute the damages he has done. Indeed, he participated in the theft of more than $1.5 million with the help of an entire criminal network. The money has been stolen from individual and corporate victims. He created multiple bank accounts in the name of a shell company in order to fool his victims. Then, the attackers sent email from an email address slightly different from the legitimate email address. The content of these emails was a payment request to the mule account. The mule and his network succeeded to launder more than $700,000 before banks froze the funds because of suspected fraud.

III. CONTROL ON THE MULE FRAUD ACTIVITIES

Mule fraud activities can come from different initial vectors. Among them, the email phishing and vishing are the preferred ones. Indeed, most of the time, they use business email compromise, which is an email that looks legitimate but contains the wrong recipient bank account. This kind of attack can be controlled by checking every email that requests a money transfer. This can be done by manually checking the recipient in the database that contains the information about the person or organization to which the money is to be sent.

The employees of the organization need to be aware of this kind of attacks. In fact, training and education can be done in the form of role-playing involving money mule attacks. Employers also need to alert employees to be aware of phishing and suspicious malware links in emails.

Employees need to recognize the signs of this kind of attacks by avoiding panicking under the pressure of the attackers. They have to be careful about suspicious emails, especially when they contain bad grammar, spelling mistakes, an urgent action request, unfamiliar greeting or salutation, inconsistencies in email addresses, links and domain names, suspicious attachments, login credentials request, payment information request, sensitive data request, and all other emails "too good to be true".

They need not to provide any sensitive information on the phone or by email, such as password, username, authentication credentials, or account information.

Another method that can be used to prevent from this kind of attacks is not to use the "reply" option when replying to an email that contains a money transfer request, instead it is better to prefer the "forward" option and writing the email address of the recipient manually, or by selecting it from a known address book (Nacha, 2021).

IV. VULNERABILITY OF THE CURRENT CONTROL TOWARDS MULE ACTIVITIES

The previously discussed way of controlling money mule fraud activities has its advantages, but it also has its vulnerabilities, if implemented alone. Indeed, checking the recipient information in the database is not sufficient since the database may have been corrupted. Attackers may have succeeded to create fake customers' accounts or modify existing ones by putting their bank information instead of the customers' ones. They may have succeeded to do this because of a malware, or any other malicious file, that may have been sent to one of the organization's computers. The attackers may have succeeded to gain administrative access in order to modify the database by escalating their privileges. This may have been done because of the organization's vulnerabilities known by the attackers, this may happen if the computers' updates are not done regularly, or if the organization is using deprecated software, or protocols. Sometimes, the administrative access is not even required since some organizations don't limit the access to sensitive data. In addition, employees may be actors of the attacks and may proceed to the payment from the company's account directly to the money mule account. Indeed, it often happens that angry employees want to take revenge of the organization and may want to do damage to it. They also may have been contacted by some criminal network that detected the irritation of the employee and may want to take advantage of it. They may ask him/her some sensitive information about the organization, they also may ask him/her to search into databases, to give them some internal access, and maybe to do

action that will allow the criminals to receive money from the organization (DeSantis et al., 2011).

V. DEFENSE TECHNIQUES TOWARD MULE FRAUD

Due to the fact that attackers may succeed to modify the customers database, it is important to secure it and secure the organization in general to avoid this case to happen.

A. GENERAL SECURITY

Some general security policies need to be implemented in the organization in order to respect regulations, protect the organization and the student data, but also the reputation of the school.

Access control is a very important subject since it defines who and how employees would be able to access data, including the most sensitive. The sensitive data needs to be strictly limited to authorized employees. It is really important because if an attacker succeed to broke into the system of the organization through the account of an employee, he will not be able to get the sensitive data if the right access control has been defined. Moreover, the computers that perform banking and accounting functions need to be isolated from other computers, so that if an attacker succeed to infiltrate the system, he will not be able to access the banking and accounting data.

Employees may also be suspects. That is why the organization needs to be very careful of its own employees. In fact, an angry employee may want to revenge and damage the organization by giving sensitive information to attackers. To prevent this kind of situations, the organization needs to apply some strict policy concerning its own employees. It should monitor each new employee, and each employee that left the company recently, as a priority. That means monitoring what the user access, what file he/she modified, created, etc… It is also very important to check the Human Resources records regularly to detect any unusual change in it, such as new customer record, or new employee records.

For each payment request received, some security procedures need to be applied. Indeed, since attackers may have corrupted the database, a dual control needs to be implemented. That means that a kind of second factor authentication needs to be added in the organization's payment process. For example, when a payment request is received from a customer, the organization needs to contact the customer in order to confirm the bank information, the nature, and the amount of the transfer. This contact needs to be secure so that the organization is sure to speak with the customer. This can be done by telephone to maximize the chances to be speaking with the right interlocutor. The telephone number should be found from another source that the one stored in the organization's customers database, such as from Internet, for example.

B. OPERATIONAL SECURITY

In order to reduce the damage on the organization, it is important to have a proper operational security. When suffering from this kind of attack, a plan is required to know what to do in this situation. In this case, it is mandatory to immediately stop all online activities and disconnect all connected computer from the network.

Second, ensure that employees know how to report this type of activity to their supervisor and to the financial institution responsible for the school's bank account. If they are contacted quickly enough, they will be able to disable online access to accounts in case the attackers managed to access the accounts online, change the bank accounts passwords, open a new bank account if required. Moreover, a bank agent may be able to review all recent financial activities and cancel suspicious transfers that have been reported as fraudulent. Finally, the bank agent will be able to say to the school if any changes of password, name of the beneficiary, PIN number have been requested as well as if confidential banking documents requests may have been done.

Next, it is important to keep a written record of all events that happen with date and time, what did the school lose, if money, or data was involved. By doing this properly, the report will be reliable to the financial institutions, agencies and other impacted organizations or individual such as students or teachers.

File a complaint with the police by giving them the report of each chronological events. By doing so, it will facilitate the procedures with the financial institution. This may also lead to a law enforcement investigation which may succeed to identify, prosecute the attackers, and maybe recover lost money.

An incident response plan is to be designed and implemented in case of computers infected by malware, or hackers that succeed to break into the organization's system. In this case, the procedures are to firstly reformat the hard drives, then reinstall the operating systems on the affected computers, to reinstall needed software. Software installation files require to be downloaded from the original website of the software vendor. If investigation needs to be performed, the reformat of the drives is not to be done since evidence might be erased by doing so(United States Secret Service, 2010) [10].

C. TECHNICAL SECURITY

It is mandatory to use anti-virus and anti-spyware software to be fully protected against this kind of attacks. The updates of these software need to be done regularly, as well as all other updates in the organization's system. This software is equipped with endpoint security systems as well as network and Internet security. They are able to detect various types of malicious executable files as well as automatically detect phishing emails among a large number of emails.

The behavior of employees has also to be analyzed and monitored. To do this, User Behavior Analytics (UBA) can be used in the organization. It consists in detecting insider threats, targeted attacks, and financial frauds by identifying users' behavior patterns and detecting unusual behavior that can lead to a threat. For example, if an employee is doing the same task every day, answering emails from the same address book, but suddenly starts to do unusual tasks out of office hours, and receiving or sending emails from/to unusual addresses, the system may detect an anomaly and will alert a manager for him/her to take actions.

It is also mandatory to encrypt all the data with a strong encryption algorithm, such as AES-encryption since it will be impossible for the attackers to crack the data. Schools are not used to use cyber security defense tools, but it is really important for them to be aware of these attacks and to adapt their defense accordingly.

VI. THREAT MODELLING

Persona non Grata (PnG) as a sample shown in Fig 2 can be used to model the threat for the organization to protect against it. Indeed, if the organization is well prepared, and know the typical portrait of the potential attacker. It will be easier for it to recognize some of the attacker characteristics. Persona non Grata on the money mule person himself/herself will applied. his/her characteristics with the aim of protecting the organization. Among them, will focus on his/her motives, job, goals, and skills.

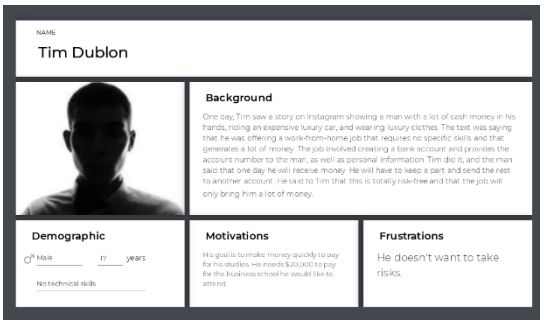

Fig. 2. Sample of Persona non grata of a mule fraudster

The PnG includes the background of the potential mule fraudster, his motivations, his frustrations, his demographic information, such as his age, gender, and skills.

The PnG tells the story of Tim Dublon, a 17-year-old high school student whose dream is to enter a prestigious business school. Unfortunately, he and his family doesn't have enough money to afford it. He is not the type of boy that will do anything for money, that is why he is not selling drugs at the moment. He wants to find a job that brings him a lot of money but without taking any risk.

A fictional story has been invented to tell the background of this person. Since it is quite common that mule fraudsters are recruited on social media (Armour, 2021), the story of Tim is that one day, he saw a work-from-home job offer on Instagram and starts doing this job to pay for his studies. His recruiters told him several times that the job was totally risk-free, and that the activity he will do is completely legal. He just needs to receive money, keep some part of it, and transfers the rest to another account. This job is perfect for Tim since it is risk-free, legal, doesn't involve a lot of complicated skills, and brings him a lot of money.

In reality, Tim is taking a huge risk because he is involved in a very dangerous criminal network and if any fraudulent activity is detected, Tim would be the first person arrested, facing a heavy fine and a long prison sentence. His accounts may also be frozen and his financial score impacted.

VII. CONCLUSIONS

To conclude, the school infrastructure is not well prepared for the increasing number of cybercrimes, the fact that the schools are not working during summer holiday doesn't help. They need to implement strong defense against these fraud crimes, and the best defense seems to be by monitoring and analyzing the behavior of the users because it takes a large number of parameters and may decide automatically to create an alert or not. This method might be helped by artificial intelligence and machine learning since the system has to learn for itself in order to take a decision.

REFERENCES

K. Rivera, C. Rohn, J. Donker, and C. Butter, "Fighting fraud: A never-ending battle," PwC's Global Economic Crime and Fraud Survey, 2020, Accessed: Dec. 03, 2021. [Online]. Available: www.pwc.com/fraudsurvey

L. Weintraub Schifferle, "What's a money mule scam?," Federal Trade Community Consumer Information, Mar. 04, 2020. https://www.consumer.ftc.gov/blog/2020/03/whats-money-mule-scam (accessed Dec. 03, 2021).

"Money Mule Awareness," Federal Bureau of Investigation - U.S. Department of Justice, Jul. 2019.

Federal Trade Comission, "Consumer Sentinel Network | Databook 2020," Nov. 23, 2021. https://public.tableau.com/app/profile/federal.trade.commission/viz/ConsumerSentinel/Infographic (accessed Dec. 06, 2021).

FBI, CISA, and MS-ISAC, "Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data," Cybersecurity & Infrastructure Security Agency, Dec. 10, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-345a (accessed Dec. 06, 2021).

FBI, "Money Mule Reined In," FBI Stories, Jul. 16, 2020. https://www.fbi.gov/news/stories/money-mule-sentenced-for-role-in-bec-scheme-071620 (accessed Dec. 03, 2021).

U.S. Attorney's Office, "Miami Man Sentenced to More Than 5 Years in Prison for Role as Money Mule and Mule Recruiter in International Cybercrime Money Laundering Network," USAO - Department of Justice, Dec. 23, 2019. https://www.justice.gov/usao-sdfl/pr/miami-man-sentenced-more-5-years-prison-role-money-mule-and-mule-recruiter (accessed Dec. 03, 2021).

Nacha, "Protecting Against Cyber Fraud | How to spot and prevent cyber fraud schemes," Nacha Fraud Booklet, Oct. 2021, Accessed: Dec. 04, 2021. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

M. Desantis, C. Dougherty, and M. Mcdowell, "Understanding and Protecting Yourself Against Money Mule Schemes," United States Computer Emergency Readiness Team, 2011, Accessed: Dec. 04, 2021. [Online]. Available: http://www.banksafeonline.org.uk/moneymule_explained.html

United States Secret Service, Federal Bureau of Investigation, Internet Crime Complaint Center, and Financial Services Information Sharing and Analysis Center, "Fraud Advisory for Businesses: Corporate Account Take Over," Oct. 2010.

Vice, "The Rise of Money Launderers on Snapchat and Instagram", Crimewave, Oct. 25, 2021. https://www.youtube.com/watch?v=UfgbZ5wJszs (accessed Feb. 25, 2022).