Comprehending Taiwan ATM Heist: From Cyber-attack Phases to Investigation Processes

Da-Yu KAO

Department of Information Management, Central Police University, Taoyuan 333, Taiwan

dayukao@gmail.com

Abstract—**Cybercriminals increasingly use sophisticated tools and advanced methods to attack bank systems. Cyber black markets for hacking tools or services are gaining widespread attention as more advanced persistent threat attacks are relevant to such markets. The recent cyber-attacks on banks or financial institutions have increased the technical expertise of cybercriminals. This study reviews ATM threats and highlights the cybercrime investigation of ATM heist. An incident investigation strategy from ISO/IEC 27043:2015 is proposed to embed cyber-attack phases and detect ATM heist. It demonstrates how this strategy can provide investigators with exceptional abilities to interpret evidence. By integrating an effective cybercrime investigation strategy, investigators can minimize the cost of collecting evidence in a forensically sound manner.**

Keyword—Cybercrime, ATM Threats, Bank Malware, Criminal Group, ISO/IEC 27043: 2015, Cybercrime Investigation, Malware Family

I. Introduction

A. *Cybercrime Threats on Sophisticated ICT environment*

The Internet has become an integral part of our society, and it enriches our lives in countless ways. Information and communications technologies (ICTs) are the integration of telecommunications, computers, and software, which enable users to access information. As the computer systems of the new ICT environment get more sophisticated than before, so do the criminals. ICTs have facilitated not only the methods in which crimes are committed but also the methods in which criminals interact in committing them.

1) Exploitable Vulnerabilities to Computer System

Zero-day vulnerabilities are exploitable weaknesses that a software vendor is not aware of and for which no patch has been created. However, half-days are also prevalent in the black market where the software creator may know of the weaknesses. A patch may be available, but few users are aware of and implementing those patches [18]. That is where the danger lies. People are the greatest threat to a computer system [8]. More exceptional care has to be paid to the individuals' authorization to access sensitive data in the computer system since this can reduce the number of attack incidents.

2) *Increasing Expertise of Cybercriminals*

The Internet has come to represent both attractive and available for finding victims. The data breach of hacking activities becomes prevalent. The sophistication of cybercriminals and their advantageous positions as attackers will target the transactions for a data breach, and innovate in ways to infiltrate computer systems [12].

3) *Undetected Cybercrimes on Malware Attacks*

Cyberspace consists of interrelated and interdependent ICT devices. That includes the Internet, telecommunications networks, and computer systems [4]. As ICT continues to change and evolve, some cybercrimes remain undetected. Cybercriminals increasingly use sophisticated tools and advanced methods to distribute a wide range of malicious attacks [6]. Cybercrimes require the advanced hacking capability to target financial services, and the global economy requires a proactive and coordinated response.

B. *Financial Technology*

Financial Technology (FinTech) refers to the use of software and digital platforms to deliver money exchange services to consumers and make it easier than ever to make transactions between two entities [21]. While much cybercrime is committed by individuals acting alone, a significant amount of criminal groups have tended to vary significantly in their criminal activities. Cybercrimes are developing exponentially and threating our FinTech. To fight against the unlimited growth of Automated Teller Machine (ATM) security threats, a sound knowledge of the problem and perpetrators can contribute to preventing cybercrimes.

1) Advantages

a) The Traditional Need for Strict Security Controls

Banks use many electronic systems for the operation of their

Manuscript received Jan. 1, 2019. This work was a follow-up of the invited journal to the accepted & presented paper of the 21st Conference on Advanced Communication Technology (ICACT2019), and this research was partially sponsored by the Executive Yuan of the Republic of China under the Grants Forward-looking Infrastructure Development Program (Digital Infrastructure-Information Security Project-109).

Da-Yu Kao is with the Department of Information Management, Central Police University, Taoyuan 333, Taiwan (Corresponding Author phone: +886-3-328-2321; fax: +886-3-328-5189; e-mail: dayukao@gmail.com).

economic environment. Traditionally, they use strict security controls overall operational and transaction-related procedures. In terms of segregation of duties, all systems administration must have dual login controls, rare network protocols, and multiple serial firewalls for internal banking communications [3]. However, banks generally choose an open system due to friendly user-interface, convenient process, or insufficient budget. That raises severe concerns on ATM protection. Several measures can be adopted by banks to detect, prevent, and minimize the cybercrime damage on the Internet.

b) Online ATMs for Convenient Payment Activities

Once computers or ATMs connect to the insecure Internet, no one can guarantee their security. Online ATMs have gained increasing popularity all over the world, as they provide convenience to the public in managing their banking accounts and payment activities [21]. The vulnerability of a complicated, fragmented ATM system relies on many providers to get customers to cash on demand. Due to the growth of FinTech, some ATM services have offered convenient payment solutions to facilitate online internal examination.

2) Disadvantages

a) The Lack of Cybersecurity Awareness

Exploits take advantage of weaknesses or vulnerabilities in software. A vulnerability run malicious code onto compromised computers. Malware can further infect other internal computers without users' knowledge [14]. Financial ATMs to internet-connected industrials should not be built using commercial operating systems for safety concerns. The lack of cybersecurity awareness may enhance the vulnerability of individuals and organizations. The threat of cybercrime impedes the development of information technology. It could contribute to the weakening of a nation's economic security.

b) Unauthorized Access of Internal ATM Details

How can the criminal group obtain the internal ATM information? Internal IP Address, computer name, and device name should be challenging to match them. As far as ICT governance is concerned, this kind of data is limited to internal vital persons. The main threat arising is the possibility of unauthorized access and use of bank card/ATM information by a fraudster [3]. Once malware is in place, buyers can rent them to deliver a variety of attacks. Active crime groups have recognized the benefits of the Internet [21]. A bank system should have the boundary of a closed system for safety concerns [10]. A closed system has no external interactions and is an isolated system that exchanges neither matter nor information with its environment. No interactions can take the form of information or material transfers into or out of the system boundary.

3) Proper Security Measures

Banks may implement several organized policies to protect against computer security threats. Moreover, banks need to provide information security training to staff, increase their awareness of the Internet dangers, and create effective practices to prevent its happening [22]. The following security measures for banks are recommended both to the cashpoints and the environment they are placed in, with sufficient lighting and cameras monitoring all activity [14].

- Review the physical security of all ATMs
- Consider investing in quality security solutions.
- Replace all locks and master keys on the upper hood of the ATMs
- Ditch the defaults provided by the manufacturer.
- Install an alarm and ensure it is in good working order.
- Change the default BIOS password.
- Ensure the machines have up-to-date antivirus protection.

The literature reviews of organized cybercrime activities and ATM threats are discussed in Section 2. Section 3 describes specific questions and behavioral attributes in Taiwan ATM Heist. An incident investigation strategy from ISO/IEC 27043:2015 is proposed to embed cyber-attack phases and detect ATM heist in Section 4. Our conclusions are given in Section 5.

II. Literature Reviews

A. Organized Cybercrime Activities

Cybercrime has grown tremendously over the past decade as public administration and private service gained a more fabulous online presence than before. The increasing risk of cyber-attack is driven by continuously changing technology, vulnerabilities, and advanced persistent threats. An ongoing chronology of serious data breaches raises awareness about cybercrime issues [16]. A review is a necessary step in the continued growth of a multi-faceted lens on cyber-attack or investigation process. The cybercrime investigation discipline intersects several fields, including computer science, criminology, and management. Cybercrime is a rapidly growing phenomenon that requires a proactive and coordinated response. The convenience for a user has become another advantage for criminals [14]. The diversity of organized cybercriminal exploits by state and non-state actors alike. Criminal offenders or nation-states have entailed a diverse set of organized activities. The following activities in Table I describe some organized cybercrime activities in recent years [7, 8].

1) Cross-broader Hackers in Organized Crime Groups

Geographical boundaries have become trivial as cyber-attacks are theoretically able to carry out from anywhere in the world. The cyber exploitations can occur outside of the reach of local Law Enforcement Agencies (LEAs)[4]. The Carberp malware source code was leaked and enhanced to create new threat products for sale to the underground fraud community [14]. The future damage cannot be limited or controlled. The do-it-yourself malware toolkit sold by the group has been used to make unauthorized banking transactions.

2) Malware Black Market for Hackers

The arrests or takedowns in cyber-attacks often lead to public media coverage. Even if a group or individual gets taken down, the vast majority of criminals do not be arrested [9]. The black market of the organized group is on the increase and often connected with crime groups or nation-states. The hackers in online black markets or dark web grow smarter as they learn from LEAs' investigative techniques. Cybercrime vendors sold access to a wide selection of malware or compromised zombies from any country. Price tags for remote desktop-based access run no more than a few dollars. The criminal group could buy access to bank employee computers that were already compromised by massively distributed opportunistic malware [14]. The international reach of LEAs has some difficulties, and the development of bank malware continued. Cybercriminals would like to hide in any particular jurisdiction and avoid prosecution. They can make use of the lucrative malware black market, raise funds for their activities, and gather intelligence on possible targets [2].

3) The Need for Profiling Hackers

Investigating hackers is a time-consuming effort. The Internet offers a degree of anonymity which affords organized crime groups the ability to recruit cross-broader hackers. The hacker forums offer criminals a wide variety of malware for low prices to assist them in criminal activities. The topic of identifying a practical framework of cybercrime investigation is a challenging one. No current set of profiling cybercriminals exists. In this regard, the emergence of a useful cybercrime investigation framework may rely on the experiences of cybercrime investigation pioneers.

TABLE I
ORGANIZED CYBERCRIME ACTIVITIES

Year	Group Name	Actor	Behavior Type	Activity
1993~2001	DrinkOrDie (DoD)	Non-state	An international group of copyright pirates	Illegally reproduced and distributed software, games, and movies over the Internet.
1996~1998	The Wonderland Club		A members-only group	Exchanged illicit images of children.
2003~	Anonymous		A decentralized group of activist and hacktivist entities.	Focus on website defacements, distributed denial of service attacks, and prominent symbols
2006~2008	Dark Market		A forum for the exchange of stolen credit card and banking details, and malicious software.	Take advantage of the criminal opportunities presented by the advent of electronic banking and the increasing use of credit and debit cards.
2006~2010	PLA Unit 61398	State	A large-scale program of industrial espionage	Acquire a massive volume of data from a wide variety of industries in English-speaking countries.
	Shady RAT		An ongoing series of cyber-attacks	Hit at least 71 organizations
	Aurora		A series of cyber-attacks	Aim at dozens of other organizations
	GhostNet		A cyber espionage operation	Operate from commercial Internet accounts in China.
2007~2013	PRISM		A systematic harvesting program of digital information by the US National Security Agency (NSA).	Capture and store a wide range of Internet data on the following prominent IT companies: Microsoft, Google, Yahoo!, Facebook, Pal Talk, YouTube, Skype, AOL, and Apple.
2009~	Lazarus, Guardians of Peace, or Whois Team		Compromised several banks and Fintech companies.	Be famous for Operation Troy, Ten Days of Rain, Sony breach, Operation Blockbuster, WannaCry, cryptocurrency attacks
2010~	Operation Olympic Games		A collaboration between the US National Security Agency and its Israeli counterpart, Unit 8200.	Disrupt the Iranian nuclear enrichment program.
	Stuxnet		A malicious computer worm is believed to be a jointly built American-Israeli cyberweapon.	Involve the clandestine insertion of a complex and sophisticated set of software into communications and control systems at the Natanz nuclear facility.
2010~2012	Ukrainian Zeus	Non-state	Software engineers in Eastern Europe	Gain access to the computers of individuals employed in a variety of small businesses, municipalities, and non-government organizations in the United States.
2016~	MoneyTaker		Stole millions from U.S. & Russian Banks	Target Banks, financial institutions, and legal firms in the United States, UK, and Russia.

B. The Shadowy Criminal Group on ATM Threats

Cyber threats are still profitable for cybercrime groups and sponsored groups, who may attack bank systems for financial profits or political reasons. Cyber risks and their follow-up losses are becoming increasingly international across the world [7]. Cybercrime investigation of these cyber threats through hacker tools, techniques, and procedures is critical for LEAs to protect users and reduce fraud risk.

Some of the most notable malware families are ZeuS (its successor Carberp) and Carberp (its successor Carbanak). The criminal's pragmatic approach starts a new chapter in the cybercrime ecosystem [14]. In this era of increasing cyber-attacks, many different malware families are programmed, especially for the majority of internet banking fraud through malware. Bank heists are attracting large-scale hackers with its unlimited borders, as cybercrime against financial banks turns out to be an increasingly convenient way to withdraw big money. This study focused on the Carberp malware, and it showed there was a grey area between APT and malware. There are a variety of shadowy criminal groups that focus on banks and payment providers. The shadowy criminal group members began actively taking an interest in retail organizations or bank payment systems. Hackers hacked up to $1 billion from more than 100 banks in 30 countries. ATM hacking is becoming a new trend for an organized cybercrime group. There are a particular tutorial, tricks, and techniques online about ATM devices hacking like Diebold, Defcon, or Wincor Nixdorf [14, 19]. It is not easy to cheat an ATM computer. If cybercrime targets financial services, it requires advanced hacking capability. Profit or money is always an initial motivation for criminals, who have targeted ATMs to withdraw cash even without the need for a card.

An organized group of criminals from Russia and Ukraine has broken into internal networks at dozens of commercial banks and installed malware that allowed the group to drain bank ATMs of cash. The ATM malware family in Latin America, Europe, and Asia are identified as 'Carberp,' 'Qadars,' 'Ploutus,' 'Tyupkin,' 'Anunak,' or 'Carbanak' during the period from 2009 to 2015 in Table II [19]. This malware has evolved and has added functionality beyond banking credential theft. The details of each malware are somewhat different. The stealthy APT methods used by the attackers in these heists would work across a broad range of commercial banks one by one. This group specializes in hacking into banks directly and then working out ingenious ways to funnel cash directly from the financial institution itself. Since 2009, researchers have warned that hackers were developing malicious software for ATMs [14]. The online banking malware of the Carberp program is reported to have impacted hundreds of financial institutions around the world since 2009. In addition to its malicious capabilities, the Carberp malware family uses a combination of evasion techniques from the Zeus malware, and the invisible persistence feature from other viruses, worms, Trojans, or botnets. Hackers can resort to open source codes to achieve their goals [13, 19]. Since 2012 several ATM heists of this type were reportedly carried out in Russia, Europe, and the USA. It appeared to be attacked by organized crime gangs, and the compromised ATMs were reprogrammed to dispense cash using malware. Ìn 2015, an international organized crime ring had stolen up to US$1 billion from more than 100 banks in 30 nations [19]. Hackers may exploit security flaws in specific ATMs, and cause the compromised machines to spew a flurry of bills on stage. Table III illustrates the behavioral comparison of the ATM malware family. These three cases were all arrested by LEAs.

TABLE II
THE FUNCTIONAL COMPARISON OF ATM MALWARE FAMILY

Malware Family	Carberp	Qadars	Ploutus	Tyupkin	Anunak	Carbanak
Identified Companies	Federal Office for Information Security, BSI and Trend Micro	Symantec, Microsoft, and Sophos	Symantec, Microsoft, and SafenSoft	Symantec, Kaspersky	Group-IB and Fox-IT	Kaspersky
Finding Time	2009	May 2013	August 2013	March 2014	December 2014	2015
Victim Location	Russian	Netherlands, France, Canada, India, Australia, and Italy	Mexico	Eastern Europe, the U.S., India, China, Russia, Israel, France, and Malaysia.	Eastern Europe, the U.S.	Russia, the United States, Germany, China, and Ukraine

TABLE III
THE BEHAVIORAL ATTRIBUTE COMPARISON OF ATM MALWARE FAMILY

Category	Case	1	2	3
Who	An organized criminal group name	Carberp, Pawn Storm or APT28	Unlimited Operations	Russian Mafia
	Suspect numbers	8	8	19
	Arrest by	Russia	USA	Taiwan
	Arrested suspects name (from Newspaper)	Germes and Arashi (Alias)	Elvis Rafael Rodriguez, Emir Yasser Yeje, and Alberto Yusi Lajud-Peña	Andrejs Peregudovs, Mihail Colibaba, and Nikolay Penkov
What	USD theft in an ATM looting	$1 Billion	$45 Million	$2.6 Million (NT$83.27 Million)
When	From plan to ATM heist	2009 ~ February 2015	December 2012 and February 2013	July 2016
	Arrest date	March 2012	May 2013	July 2016
Where	ATM location	Moscow in Russia	New York in the USA (More than 24 countries)	Taipei City, New Taipei City, and Taichung in Taiwan
How	Money from	the financial institution	Prepaid Debit Accounts	the financial institution itself

III. SAMPLE CASE: TAIWAN ATM HEIST

In recent years there has been a tremendous increase in organized crimes. Banks in many countries are becoming new targets of several independent cybercrime groups. Traditional organization crimes have a hierarchical top-down command-and-control structure, but cybercrime groups tend to involve a loose network or even a peer-to-peer decentralized structure [1]. The group operated in closed cells, and the suspects did not know each other involved in the ATM heist [14]. These attacks rely upon both highly sophisticated hackers and criminal cells whose role is to withdraw the cash as quickly as possible. The crime chain is the series of steps cybercriminals go through to transform its ATM invasion into something of higher value. They make their output worth more than the sum of its inputs.

A. Specific Questions in Taiwan ATM Heist

The ATM transactions in the USA's Unlimited Operations require only general bank card information to effect payment, such as the bank card number, and PIN code [19]. However, Taiwan's Russian Mafia Group in July 2016 further compromises the ATM systems and criminals can withdraw money without any bank card information. The ATM heist of Taiwan First bank is based on a well-known Carberp malware family, which is available for sharing, sale or cooperation on such markets. Investigators seek to explore cyber-attacks. The arrest was made after police officers spent many sleepless nights watching surveillance videos and checking hotel registries in Taiwan. Putting relevant data all together becomes essential to support or refute a cybercrime. The questions go along the lines of whom, who, how, and why [13, 20, 23]. Without understanding these root causes, it would be difficult to use evidence from multiple independent sources, develop a strong association between a criminal and an event, and explore the incident under control.

1) Who Are Victims?

The ATM attack in Taiwan targeted the First Bank's network. The ATM heist occurred between July 9 and 10 2016, when members of ATM heist gangs stole over USD 2 million from 41 ATMs in Taipei, New Taipei and Taichung using malware to hack into the computer system [15]. The Wincor Nixdorf ATM framework was targeted. They use malicious software and defy the bank effort to strengthen the security controls of ATM fleets. That case has demonstrated that bank systems lack adequate security measures to stop cybercrimes.

2) Who Are Cybercriminals?

Three cybercriminals were arrested on July 17, 2016, and each was sentenced to prison terms of 12 years. The 19 escaped cybercriminals have been put on a wanted list, and a total of 22 cybercriminals from six countries were involved [15].

3) How Did Hackers Do?

The heist was committed without using cards, but the ATMs spat out bills. LEAs have identified some patterns to trigger withdrawals. As a result of access to internal bank networks, hackers also gained access to ATM systems, infected these computers with their specific malware, and launched the fraud command from London, UK. The dispensing of the cash could have been triggered by a mobile phone, a laptop, or a hacked private bank computer. The cybercriminals use Whatsapp and other Internet-based communication methods to communicate internally and with other criminal cells [15]. They used an old spying technique of dead drops and modern technology to move the stolen money around. A dead drop is a method of espionage tradecraft used to pass items or information without meeting each other directly. Another method of a live drop is used when two persons meet to exchange items or information.

4) Why Did this Attack Happen?

Organized criminals can rent hackers to conduct attacks or hire mediators to handle the sale of stolen information. Cybercrime as a service (CAAS) increases when the ATM malware is sold to the highest bidders. Criminals no longer need to rely on their knowledge, abilities, and abilities to carry out exploits, build threats, and launch attacks. This ATM malware is sold only to selected people. Most of the infections are from a different group and share the command and control (C&C) servers [13]. The profit attracts hackers by running vulnerable services. Cybercriminals try to maximize their financial gain while minimizing their risk [2].

B. Behavioral Attributes of ATM Malware Family

In several historical data breaches, hackers have exploited security flaws in specific ATMs, and cause the compromised machines to spew a flurry of bills on stage. The behavioral comparison of the ATM malware family is listed in Table IV [13, 19]. Their local LEAs arrested these three cases. In March 2012, the 8-member arrest of Department K group in Moscow by the Russia Ministry of Internal Affairs (Министерство внутренних дел) was a great example of international collaboration between both private industry research and international law enforcement (see the case 1 in Table IV). A lack of awareness of cybersecurity may enhance the vulnerability in the public or private sectors. Their differences are likely due to the type of cybercrime victimization, the effectiveness of cybersecurity measures, or the extent of online banking services. Unlike the traditional forms of crime, cybercrimes can act without leaving a fingerprint for their actions. Not only the Internet but also commercial bank systems are facing increasing physical and virtual risks [17].

TABLE IV
THE BEHAVIORAL ATTRIBUTE COMPARISON OF ATM MALWARE FAMILY

Category		1	2	3
Case	An organized criminal group name	Carberp, Pawn Storm or APT28	Unlimited Operations	Russian Mafia
	Arrest by	Russia	USA	Taiwan
	Arrest date	March 2012	May 2013	July 2016
Physical	Criminals under arrest	V	V	V
	Shadowy criminal group	V	V	V
	Assistance from other countries' LEAs		V	
	On-premises to withdraw cash	V	V	V
Virtual	32-bit Windows ATM platforms	V	V	V
	Through the ATM's pin pad		V	
	No user account required	V	V	V
	On-Premises to install the malware		V	
	Avoiding detection	V	V	V

Note: 'V' means match.

1) Access Controls

The ATM operation is continuing to become more complex, challenging, and costly. Most ATMs are still running Windows XP, which is first released on October 2001. When Microsoft has ended support for Windows XP, most ATM manufacturers continued to use this version [19]. The old system often opens security holes for hackers. There will be a persistent increase in ATM robbery around the world. The access controls of ATM theft still leave much to be desired. They are networked devices that have many potential weaknesses if not carefully configured, updated, and physically secured. It is vital to improving the security controls within banks. Although security controls can never be perfect for implementing and expensive to deploy, it remains of critical importance for security measures to be continually managed, reviewed, and improved. Insufficient budget can never be used as the reason for not taking action [21]. The default setting for any users is no or limited access. If nothing has been correctly configured for an individual or the groups, users should not be able to access that resource. Banks should enforce strict access criteria, and pay more attention to limiting and monitoring the usage of administrator and other privileged accounts.

ATMs need remote access to communicate with bank data, so network attacks are also a possibility [14]. A trade-off between convenience and security lies in wireless communication over the public Internet or dedicated connections. If convenience increases, security must decrease. The availability of access to bank ATMs from internal network segments opens excellent opportunities for hackers. Security holes or mistakes of a system configuration in the internal bank network left sensitive databases exposed to hackers. The strategy should remove or limit the remote access for ATMs.

2) Physical Process

a) Criminals under Arrest

Three organized criminal groups were arrested in Russia, USA, and Taiwan. They were involved in large scale ATM jackpotting. Their methods of operation were similar to each other.

b) Shadowy Criminal Group

The group allegedly used a piece of malware, pilfered cash from ATMs, and made millions by infecting ATMs across the world.

c) Assistance from other Countries' LEAs

It is difficult for any country to expand its power to other countries. The cybercrime arrest needs assistance from other LEAs. Arrests often take years because the cybercriminals were located in countries where the local authorities would not arrest them.

d) On-Premises to Withdraw Cash

LEAs can theoretically catch criminals in the act with security cameras since they must be on-premises to withdraw cash. However, it is difficult to obtain relevant evidence and differentiate a criminal and a regular customer.

3) *Virtual Process*

a) 32-bit Windows ATM Platforms

ATM malware worked on ATMs that run Windows 32-bit operating systems.

b) Through the ATM's Pin Pad

With the help of ATM malware, cybercriminals were able to empty the infected ATM cash cassettes by issuing commands through the ATM's pin pad.

c) No User Account Required

The malware allows its operators to withdraw cash from ATMs without the requirement of any payment card.

d) On-Premises to Install the Malware

Cybercriminals started by unlocking an ATM's enclosure and infected the computer with a piece of malware. Days later, they returned to the computer and dispensed from the ATM without the need for user account verification.

e) Avoiding Detection

The ATM malware kept the exploit hidden most of the time and had several features that helped it avoid detection [13]:

- It was only active at specific times of the night on certain days of the week.
- ATM malware implements anti-debug and anti-emulation techniques
- The malware could disable the anti-virus system from the infected system.

IV. Comprehending Taiwan ATM Heist: from Cyber-attack Phases to Investigation Processes

A. Embedding Cyber-attack Phases into the ATM Heist Investigation

According to public reports surrounding the incident investigation of Taiwan ATM heist, criminals deleted traces of the cyber-attack to prevent from detecting irregularities in the ATM behavior. Some malware behaviors and file names have been identified from the cyber-attack phases [14, 15, 19, 24].

1) Reconnaissance and Footprinting

In this phase of reconnaissance and footprinting, criminals gather information about computer systems, reveal system vulnerabilities, and find ways to intrude into the cyberspace [18]. Most exploits are dependent on operating systems, applications, ports, or services. Hackers may perform reconnaissance for about 2 to 3 times to gather a big-picture view of a network or servers before they attempt an exploit. It identifies the IP addresses, open ports, running services, and operating systems in the target network [22, 24]. Footprinting identifies the operating system, service pack or patches of the target, gathers the maximum information about the computer system or a network, evaluates the security of any IT infrastructure, and determines the follow-up attack path. It is used to get detail information on a specific target. For example, if a server is listening on port 80, it is running the HTTP protocol and is very likely a web server. It is often used as part of a more significant reconnaissance attack. Increased access to the Internet has enabled cybercriminals to perform reconnaissance on their targets. Cnginfo.exe and cnginfo_new.exe can read the information inside the ATM in the phase of reconnaissance and footprinting.

2) Scanning or Enumeration

In this phase of scanning and enumeration, hackers gather in-depth information on the victims. Enumeration often occurs after scanning [17]. The more hackers know in advance, the fewer surprises they will have. They run scanning activities to infer vulnerabilities on the Internet. Once a computer is found vulnerable, they attempt to control or infect that computer based on the inferred vulnerability. Running a ping sweep or a network mapper can explore what systems are on the network. Running a vulnerability scanner can also determine which ports may be open on a particular system. Enumeration refers to actively connecting to a target system, and identifies usernames, computer names, network resources, shares, and services. It also refers to actively connecting to a target system to acquire this information. Once a vulnerability is identified, a cyber-attack is relatively easy to disguise. There is no clear evidence from criminals' scanning or enumeration. These activities can be found from the target's firewall log files. Auditing logs can be monitored to detect threatening incidents promptly. By monitoring logs of digital evidence, LEAs can look for the triggers or something suspicious.

3) Gaining Access

In the phase of gaining access, these attacks can access insecure access [18]. Hackers can gain access to the system, crack a password, and escalate privileges. The hackers initially compromised a vulnerable telephone recording computer used by the targeted bank in order to establish network access. Cngdisp.exe and cngdisp_new.exe potentially contain more robust capabilities than cngdisp.exe, executed the function of dispensing bills in the phase of gaining access.

4) Maintaining Access

Gaining access to a connection does not mean hackers can access everything. The objective of maintaining access is to ensure that hackers can have long-term access. Hackers used this network access to move laterally within the targeted bank's network and subsequently gained access to deliver software updates across the network. They use the update service to send malware to the target ATMs. The malware masqueraded as a software update. They utilized the remote commands to empty the cash-carrying cassettes in the infected ATMs. There was no action required at the ATM except the collection of the money.

5) Covering Tracks

In the final phase of covering tracks, hackers attempt to conceal their trails, manipulate the event logs, and avoid detection by the system administrator or LEAs. Log files contain information about every computer activity. Hackers may try their best in hiding or obscuring the applications they leave behind. That leads hackers into paying attention to log files. Covering tracks consists of removing or altering log files, hiding files with unclear attributes, or using tunneling protocols to communicate with the information system [18]. Hackers need to evade detection, erase evidence of a compromised computer, and remove the portions of logs that can reveal their presence. A significant amount of malware deploys various anti-forensics tricks in an attempt to make the analysis more difficult. In the final phase of the cyber-attack, the criminals deleted (sdelete.exe) components of the malware employed in the ATM heist. Sdelete.exe and batch file cleanup.bat deleted the other programs in the phase of covering tracks [15].

B. Detecting ATM Heist Using ISO/IEC 27043:2015 Incident Investigation Processes Classes

The regulation of cyberspace law often lags behind technological development in cybercrime. Hackers will try their best to hide their identity and reduce their chances of detection across jurisdictional broader. A threat determines the risk, but for each risk, LEAs can determine the following countermeasures. The cybercrime investigation processes in ISO/IEC 27043:2015 are purposely designed at an abstract level for different types of cybercrimes [11]. In Table V, the cybercrime investigation processes in cyber-attack scenarios from LEAs' perspective can be further discussed and analyzed into the following processes classes: Readiness, Initialization, Acquisitive, Investigative, and Concurrent.

TABLE V
CYBERCRIME INVESTIGATION FROM ISO/IEC 27043:2015

Processes Class	People	Process/Activities	Technology
Readiness	System administrators	Pre-incident investigation/ plan and prepare	ICT Governance
Initialization	First responders	Cybercrime investigation/ respond	Live forensics
Acquisitive	Lab analysts	Physical investigation/ identify, collect, acquire, and preserve	Dead forensics
Investigative	LEAs	Event reconstruction/ understand, report and close	Digital forensic analysis
Concurrent	Obtaining Authorization Process, Documentation Process, Managing Information Flow Process, Preserving Chain of Custody Process, Preserving Digital Evidence Process, and Interaction with Physical Investigation Process		

1) Readiness Processes Class: Prepare the ICT Governance from System Administrators

The first class of readiness processes is prepared in advance for an investigation. Investigators can plan incident detection, identify potential digital evidence sources, analyze digital data, and explore the truth in a legally proper way. This class deals with pre-incident investigation processes and ensures that incident detection systems are in place [5]. Deploying a digital forensic readiness program can favorably impact LEAs by maximizing the potential of digital evidence and minimizing the time and costs of an investigation [11]. The investigators of data breaches can initiate some plans for taking the actions, reinforces a direct relationship between cybercrime investigation and fact-finding. Cybercrime prevention requires the participation of Internet users, the system administers, or enterprises to maintain personal or commercial data. The whole society should be encouraged to participate more fully and effectively in cybercrime prevention in order to provide for a harmonious online world [21]. A supplementary strategy is intended to achieve the goal of information security. This method can assist banks or LEAs in dealing with today's ever-increasing ATM heist.

2) Initialization Processes Class: Initiate the Live Forensics from First Responders

The second class of initialization processes deals with uncovering the potential digital evidence and searching for traces of digital evidence in a legal process. It includes incident detection, first response, and preparation [11]. The implementation of cybercrime investigation procedures includes the responsibilities for establishing a direction for its execution. The identification of appropriate best practices should develop a cybercrime investigation strategy, implement risk management, and meet the need for an investigation with acceptable efforts. There is an opportunity to actively collect potential evidence in the form of log files or network traffic records in a forensically sound manner. Live forensics primarily targets volatile data from a running system. Ignoring the volatile data of computer memory is impossible in collecting digital evidence. It can be the first step toward an incident response scenario. Live forensics can analyze volatile data, system running processes, cached processes, network connections, and opened ports without shutting down a system. Practitioners can directly make contact with the suspect and ask what has happened. Investigators can locate, extract, and analyze data from digital devices, which LEAs interpret to serve as legal evidence [16].

3) Acquisitive Processes Class: Perform the Dead Forensics from Lab Analysts

The third class of acquisitive processes deals with the physical investigation of a case where potential digital evidence is identified and handled. It includes identification, acquisition, transportation, and storage in potential digital evidence [11]. In dead forensics, practitioners can conveniently minimize system modification when working with a copy of a write-protected drive at laboratories. An examination of the computer is conducted systematically to ensure the admissibility of the evidence. The investigator should achieve continual improvement of the cybercrime investigation and take reactive activities based on the results of the case reviews or other relevant information. The investigation procedure will continue to evolve together with the requirement to incorporate new evidence and associated knowledge. LEAs have actively gathered evidence to support a legal defense [23].

4) *Investigative Processes Class: Conduct the Digital Forensic Analysis from LEAs*

The fourth and last class of investigative processes develops a likely sequence of events. It includes investigating the incident, analyzing the evidence, interpreting results from the analysis, and reporting on results of the digital evidence. Investigators can examine the pieces of evidence to measure performance against the determined objectives and report the results to the appropriate recipients for review. A singular strategy can not resolve the majority of cybercrime challenges. Technical minds alone cannot solve the issue of prosecuting cybercriminals. Given limited time and resources, it is essential to maximally leverage knowledge, capabilities, and investments in a range of public-private partnerships to improve foundations of trust and enhance agility and resilience.

5) *Concurrent Processes Class: Take Place in Company with these Processes Classes*

The following concurrent processes class takes place in company with the former processes classes [5, 11, 20].

a) Obtaining Authorization Process

Having authorization from the appropriate authorities makes sure that the appropriate countermeasures are ready to solve it.

b) Documentation Process

Investigators must maintain documentation of digital evidence from the beginning of the e-discovery process until the end.

c) Managing Information Flow Process

Information flow could describe the use of trusted PKI and time stamping to identify the exchange of digital evidence between each of the processes in the same investigation.

d) Preserving Chain of Custody Process

The documentation comprises the chain of custody form and records relating to the evidence analysis.

e) Preserving Digital Evidence Process

In order to preserve the integrity of the digital evidence, investigators should guarantee that the original evidence is not changed.

f) Interaction with Physical Investigation Process

There are some complex interactions with the physical investigation according to the digital investigator's needs and fast adaption to changing boundaries, scope, or investigation objectives. All of the complexities must be simplified to ensure an efficient investigation.

V. CONCLUSIONS

ICT innovations are not only set to bring enormous benefits to the general public, but also bring new technological risks to individuals and businesses. Cybercrimes have rapidly evolved for the dissemination of malware. Criminals increasingly use sophisticated tools and methods to commit their cybercrimes. Major information systems of modern society are under the burgeoning attack. Cybersecurity for banking or financial institutions becomes a vital business enabler to enhance customer confidence and bring in more business. It is vital to leverage investments in a range of societies to assure societal services. The ATM withdrawals happened so quickly that none of the commercial banks involved noticed in time to stop the perpetrators. ATM technologies are evolving fast and making payments more convenient. Organizations need a balance between security and functionality in information security. This study outlines a set of profiling cybercrime investigation that aims to identify digital pieces of evidence in the face of increased complexity and vulnerability in hacking activities. It is our sincere hope to bring the technical details to the attention of information security specialists and to minimize risks by preventing information security incidents. A small sacrifice inconvenience can be useful to prevent an attack on the ATM's door. ICT governance should be employed by banks to heist ATM money with more barriers.

REFERENCES

[1] Ablon, L., Libicki, M. C., and Golay, A. A. *Markets for Cybercrime Tools and Stolen Data Hackers' Bazaar*, Rand Corporation, pp. 3-28, 2014.

[2] Akhgar, B., Staniforth, A., and Bosco, F., *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Elsevier Publishing, pp. 88-90, 2014.

[3] Bates, A. and Hassan, W. U., "Can Data Provenance Put an End to the Data Breach? " *IEEE Security & Privacy*, Vol. 17, No. 4, pp. 88-93, July-Aug. 2019.

[4] Bernik, I., *Cybercrime and Cyberwarfare*, John Wiley & Sons Inc., pp. 1-57, 2014.

[5] Brooks, C. L., *CHFI Computer Hacking Forensic Investigator Certification All-in-One Exam Guide (1st Edition)*, McGraw-Hill Education, pp. 13-50, 2015.

[6] Casey, E., *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd Edition)*, Elsevier Inc., pp. 187-306, 2011.

[7] Coburn, A.W., Daffron, J., Smith, A., Bordeau, J., Leverett, É., Sweeney, S., and Harvey, T., "Cyber Risk Outlook 2018, " Centre for Risk Studies, University of Cambridge and Risk Management Solutions, Inc., pp. 2-25, 2018.

[8] Europol and European Cybercrime Center, "Internet Organised Crime Threat Assessment (IOCTA) 2018, " European Union Agency for Law Enforcement Cooperation, pp. 14-65, 2018.

[9] Graves, M. W., *Digital Archaeology: The Art and Science of Digital Forensics*, Addison-Wesley, pp. 91-110, 2014.

[10] Impagliazzo, J. and McGettrick, *A., Information Systems: What Every Business Student Needs to Know*, NW: Taylor & Francis Group, 2016.

[11] International Organization for Standardization (ISO), "ISO/IEC 27043:2015 Information Technology - Security Techniques - Incident Investigation Principles and Processes," ISO Office, 2015.

[12] Jewkes, Y, and Yar, M., *Handbook of Internet crime*, Willan Publishing, pp. 173-193, 2009.

[13] Kao, D. Y., "Exploring the Cybercrime Investigation Framework of ATM Heist from ISO/IEC 27043:2015, " IEEE ICACT 2017 (19th International Conference on Advanced Communications Technology), Pyeong Chaung, South Korea, 2017.

[14] Kao, D. Y., "ATM Heist Threats: a Proposed ICT Governance Strategy," IEEE ICACT 2019 (21th International Conference on Advanced Communications Technology), Pyeong Chaung, South Korea, pp. 610 - 615, 2019.

[15] Law and Regulations Retrieving System, "Criminal Appeals No. 593/106 in Taiwan High Court," Judicial Yuan, May 18, 2017.

[16] Marcella, A. J., Menendez, D., *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes (2nd Edition)*, Auerbach Publications, pp. 1-26, 2008.

[17] Mehan, J. E., *Cyberterror, Cybercrime, and Cyberactivism: An In-Depth Guide to the Role of Security Standards in the Cybersecurity Environment (2nd Edition),* IT Governance Publishing, pp. 25-58, 2014.

[18] Oriyano, S. P., *CEH v9: Certified Ethical Hacker Version 9 Study Guide (3rd Edition)*, John Wiley & Sons, Inc., pp. 1-222, 2016.

[19] Sancho, D., Huq, N., and Michenzi, M., "Cashing in on ATM Malware: A Comprehensive Look at Various Attack Types," Trend

Micro Forward-Looking Threat Research (FTR) Team and Europol's European Cybercrime Centre (EC3), 2017.

[20] Shipley, T. G. and Bowker, A., *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Elsevier Inc., pp. 21-38, 2014.

[21] Smith, R. G., Cheung, R. C. C., and Lau, L. Y.C., *Cybercrime Risks and Responses Eastern and Western Perspectives*, Macmillan Publishers Limited, pp. 67-211, 2015.

[22] Spitzner, L., *Honeypots Tracking Hackers*, Addison-Wesley, pp. 8-20, 2002.

[23] Stephenson, P., *Official (ISC)$^{2®}$ Guide to the CCFP CBK*, Auerbach Publications, pp. 293-404, 2014.

[24] Walker, M., *CEH Certified Ethical Hacker All-in-One Exam Guide (2nd Edition)*, Graw-Hill Education, pp. 35-198, 2014.

Da-Yu Kao received the B.S. and M.S. degree in Information Management from Central Police University, Taiwan, in 1993 and 2001, the Ph.D. degrees in Crime Prevention and Correction from Central Police University, Taiwan, in 2009, respectively. From 1993 to 1996, he was with Taipei City Police Department, Taiwan, where he was an information technology police officer involved in the development of policing information systems. From 1996 to 2007, he was with Criminal Investigation Bureau, National Police Administration, Taiwan, where he was a detective and forensic police officer in cybercrime investigation and digital forensics. From 2007 to 2013, he was with Maritime Patrol Directorate General, Coast Guard Administration, Taiwan, where he was an information technology section chief in the department of information and communication. Since 2013, he has been with Central Police University, Taiwan, where he is currently an associate professor in the Department of Information Management. His research interests include cybercrime investigation, digital forensics, digital evidence, information management, criminal profiling, and cyber criminology.