The Wild Robbing of Online Bank: Financial Crimes and Digital Forensics

Associate Professor Dayu Kao (Ph. D.)
Department of Information Management,
Central Police University, Taiwan
camel@mail.cpu.edu.tw

Governance
People, Process, and Technology

- **People: Employee Awareness**
  - **Custom service**
  - **De-identification** is the process used to prevent someone's personal identity from being revealed.
  - **Personal Info**
- **Process: PT, Black Box, …**
- **Technology: Mobile Bank, SQL Injection, …**
- **Limitation: Law, Regulation, Policy**

第一銀行
First Bank

遠東商銀
Far Eastern International Bank

The Four elements of Auditing Logs in Cyber-crime Investigation

No	4 Elements	Tier-1	Tier-2	Tier-3
1	IP Address	Which sources are identified and obtained from the available logs?	Where is the computer locate?(One computer or two)	Who is s(he)?
2	Time Stamp	When is the period between start time and end time?		
3	Digital Action	What are (ab)normal results?	Why was the crime committed?	
4	System Messages	How are the actions recorded? (Successfully or failed)		

IP Address Types

- Static IP Address: web address content is the same all the time and is managed or used by specific organization such as www.cib.gov.tw, bbs.csie.nctu.edu.tw
- Dynamic IP Address: used by different people during different time (specific time for specific people), located specific location such as h135.s95.ts.hinet.net(168.95.95.134), as1po2.ks.ficnet.net.tw(202.145.188.130)
- Proxy IP Address: No log files available from ISP, and more information are necessary such as 168.95.0.6(tpproxy6.hinet.net)

Inquiry Types from Log

- Email address：e-mail:camel@mail.cpu.edu.tw
- Webpage (website) address：
  http://bank.ucs.com.tw/gift/default.html
- Fixed time dynamic IP address：
  - h159.s90.ts32.hinet.net at 13 Jun 1999 11:38:17 +0800
  - h159.s90.ts32.hinet.net at 12 Jun 1999 23:38:17 -0400(13 Jun 1999 11:38:17 +0800）
- Proxy address origin inquiry：proxy6.hinet.net at 13 Aug 2007 04:12:00 –0400(16:12:00 +0800) to www.cga.gov.tw
- Single account connection log：connection record of Amy on 2010 Jan 20th

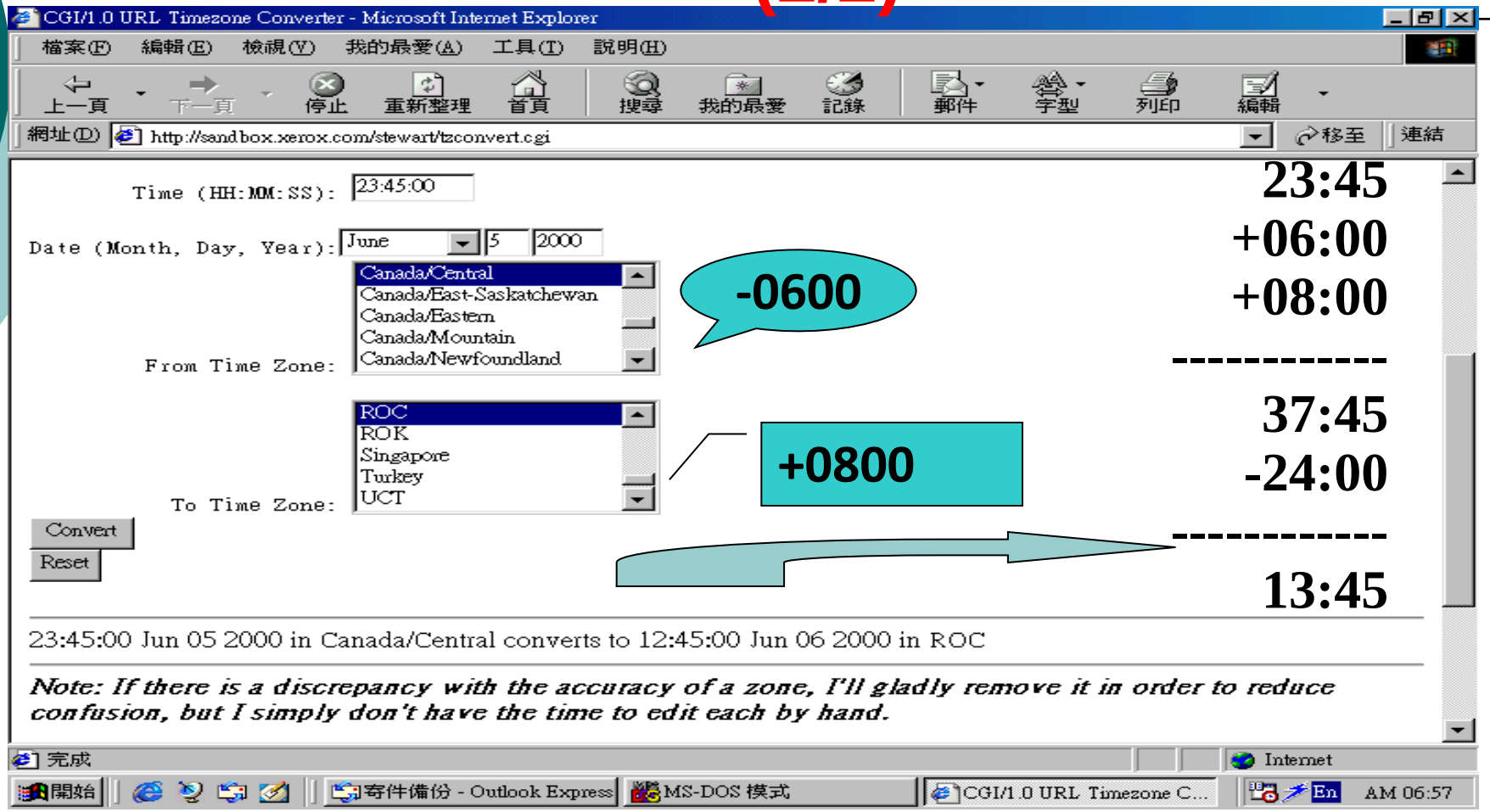
ISP Inquiry

- International
  - http://www.whois.sc/
  - http://www.allwhois.com/
  - http://whois.namespace.org
- Taiwan
  - http://www.whois.twnic.net/
  - http://rs.twnic.net.tw/

First Rule on Investigation: Time Check (1/2)

- Check time zone: click on lower right corner of WINDOW and select your time zone
- Often seen time zones: notice the daylight saving time
  - GMT is +0000
  - CST is +0800
- Time zone conversion: the following times are the same time
  - Jul 7 04:00:00 –0800
  - Jul 7 12:00:00 GMT
  - Jul 7 20:00:00 +0800

Time Zone Converter – Daylight Saving Time (2/2)



http://www.timezoneconverter.com/cgi-bin/tzc.tzc

Daylight saving Time /Time Zone Converter

Bank robbery

- Bank robbery is the crime of stealing money from a bank, specifically while bank employees and customers are subjected to **force, violence, or a threat of violence**.
- According to the Federal Bureau of Investigation's Uniform Crime Reporting Program, robbery is "the taking or attempting to take anything of value from the care, custody, or control of a person or persons by force or **threat** of force or **violence** or by putting the victim in **fear."**
- By contrast, burglary is "**unlawful entry** of a structure to **commit a** felony or **theft**."

https://en.wikipedia.org/wiki/Bank_robbery

Early examples

- According to The New York Times and the Saturday Evening Post, the **first bank robbery in the United States** occurred in March 1831 (the 19th according to the Times, the 20th according to the Post).
- Two men, James Honeyman and William J. Murray, entered the City Bank of New York **using forged keys**. This allowed them to **empty the vault** of more than $245,000 in bank money.

Insider(s)?

Stockholm Syndrome

- In 1973, four hostages were taken during the Norrmalmstorg robbery in Stockholm, Sweden. After their release, the hostages (victims) **defended their captors (criminals)** and refused to testify against them.
- This led to an academic interest in a phenomenon soon after referred to as **Stockholm syndrome**, wherein hostages, during captivity, paradoxically form a sympathetic bond with their captors as a survival strategy.

Testify against the cybercriminal?

Higher Arrest Rates on Continuous crimes

- The police have new measures to catch bank robbers.
- Forensic identification techniques have also improved greatly but are not particularly effective in some cases.
- While it is not certain that the first time someone robs a bank online they will be caught if they continue to rob banks, they will most likely be caught.

Effective prevention? Whose help?

Cyber Crime Continues to Plague Banks and Bank Customers

- Thursday, July 11, 2019

- Regulatory concerns are increasing as banks turn to FinTech partners to provide technology to compete with money transfer and other services.
- Banks should constantly be aware of and monitor the increase in vendor security risks and must be proactive in investigating the security processes of vendors.
- Both financial institutions and their customers should ensure proper cyber liability coverage.
- With the **increasing cyber risks and increasing potential liability and lost income**, it is imperative to educate customers as to the risk of a Business Email Compromise (BEC)/Email Account Compromise (EAC) attack.

Cyber Bank Robberies Contribute to $1 Trillion in Cybercrime Losses

- Bank robbing is an age-old crime and remains a nasty business. The banks will pass their losses on to consumers.
- Today, bank thefts are done digitally and with a lot more finesse and stealth than in days-gone-by.
- It still costs everyone dearly as it's a daily occurrence.

https://www.globalsign.com/en/blog/cyber-bank-robberies-contribute-to-1-trillion-in-cybercrime-losses/

The Wild Robbing of Online Bank

Profit-oriented **Profit > Risk**

- Why do they do it? It's lucrative and relatively low risk in terms of detection. This is inspiring even more criminals to "go online."
- While some groups break up or are caught by the cyber-police, newer groups turn up with more sophisticated attack techniques to take their place.
- Turns out that these criminals quickly adapt to the changing environment. They are constantly monitoring for the latest weaknesses and pounce on them much faster than security officials can patch in updates.

Some examples of the cyber-banking crimes

- Theft of $100 million - in early 2017, there was a surge of attacks targeting card processing in Eastern Europe.
- Theft of $60 million - in the fall of 2017, intruders attacked the SWIFT of Far Eastern International Bank in **Taiwan** by making transfers to accounts in Cambodia, Sri Lanka, and the US.
- Theft of $4 million - while banks in Nepal were closed for holidays, criminals used SWIFT to withdraw money.
- The banks were able to track transactions and recover a significant portion of the stolen funds only due to timely response.

Some examples of the cyber-banking crimes

- Theft of $1.5 million - in early December 2017, in Russia and in the United States for a year and a half.
- Criminals attacked card processing and inter-bank transfer systems, with thefts averaging $500,000 in the US and RUB 72 million (~$1.26 million) in Russia.
- Theft of $100 thousand – also in December 2017, the first successful SWIFT attack on a Russian bank.
- The victim of the hacking attack was Globex, a subsidiary of **state-owned Vnesheconombank (VEB)** bank.
- The suspect is the Cobalt **hacker gang**, which specializes in cyber-attacks on banks.

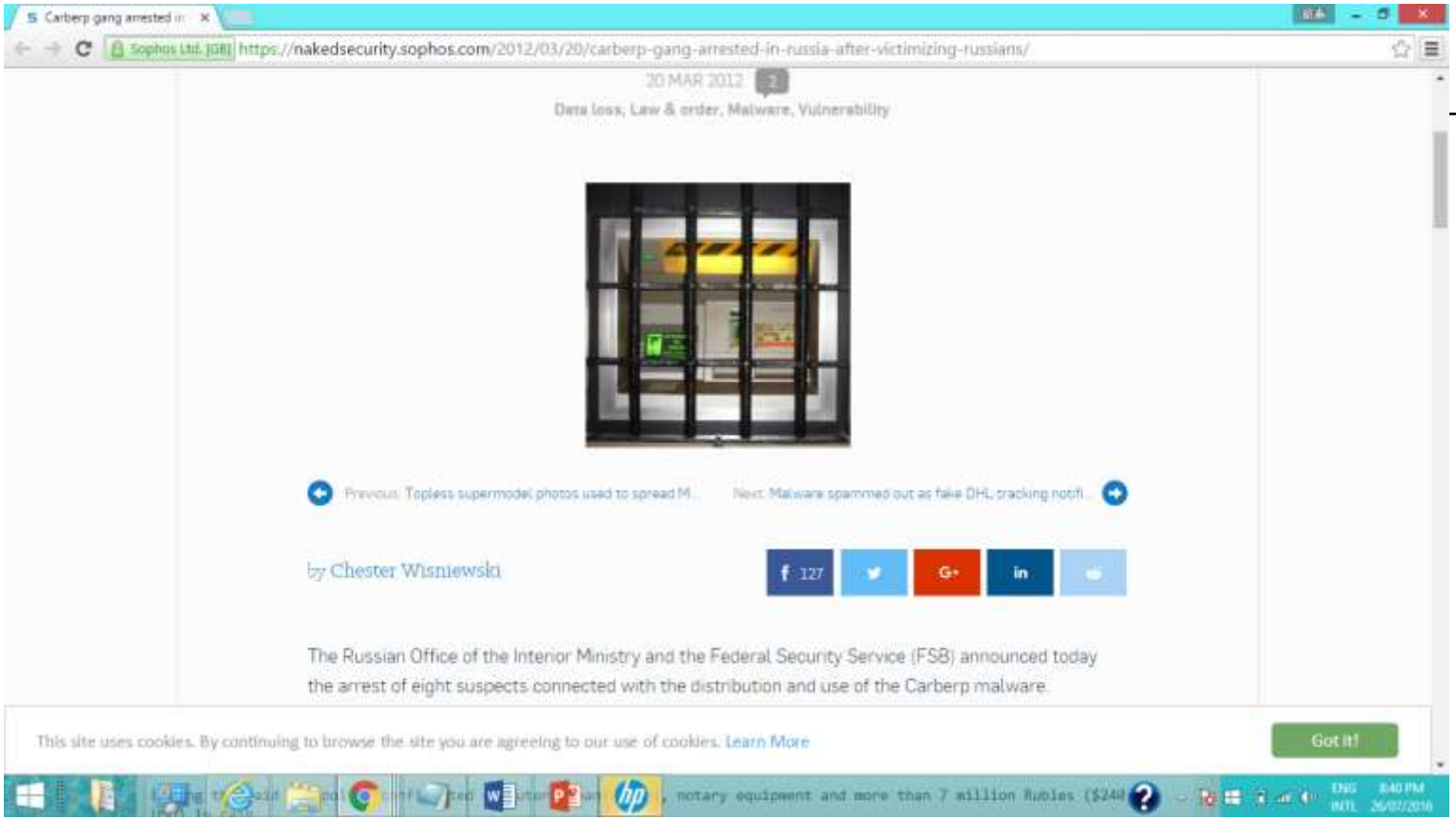
Hacked financial industry in Taiwan

- **April 2010**: Yushan Bank was invaded by hackers using Trojan horse programs, more than 16,000 customers were leaked, and no account was stolen. (Be fined 4 million NTD)
- **July 2016**: First Bank's ATM theft case, the hacker used the telephone recording system of a Bank London Branch as a springboard, and finally remotely controlled 41 One Bank ATMs across Taiwan, stealing more than 83.27 million NTD. Most of the money has been recovered return
- **September 2016**: First Bank and First Gold Securities were attacked by a hacker to conduct a decentralized blocking service attack (DDoS). The services of personal online banking, enterprise gold online banking, and securities dealers' electronic ordering platforms were interrupted for several hours.

ATM Heist Threats

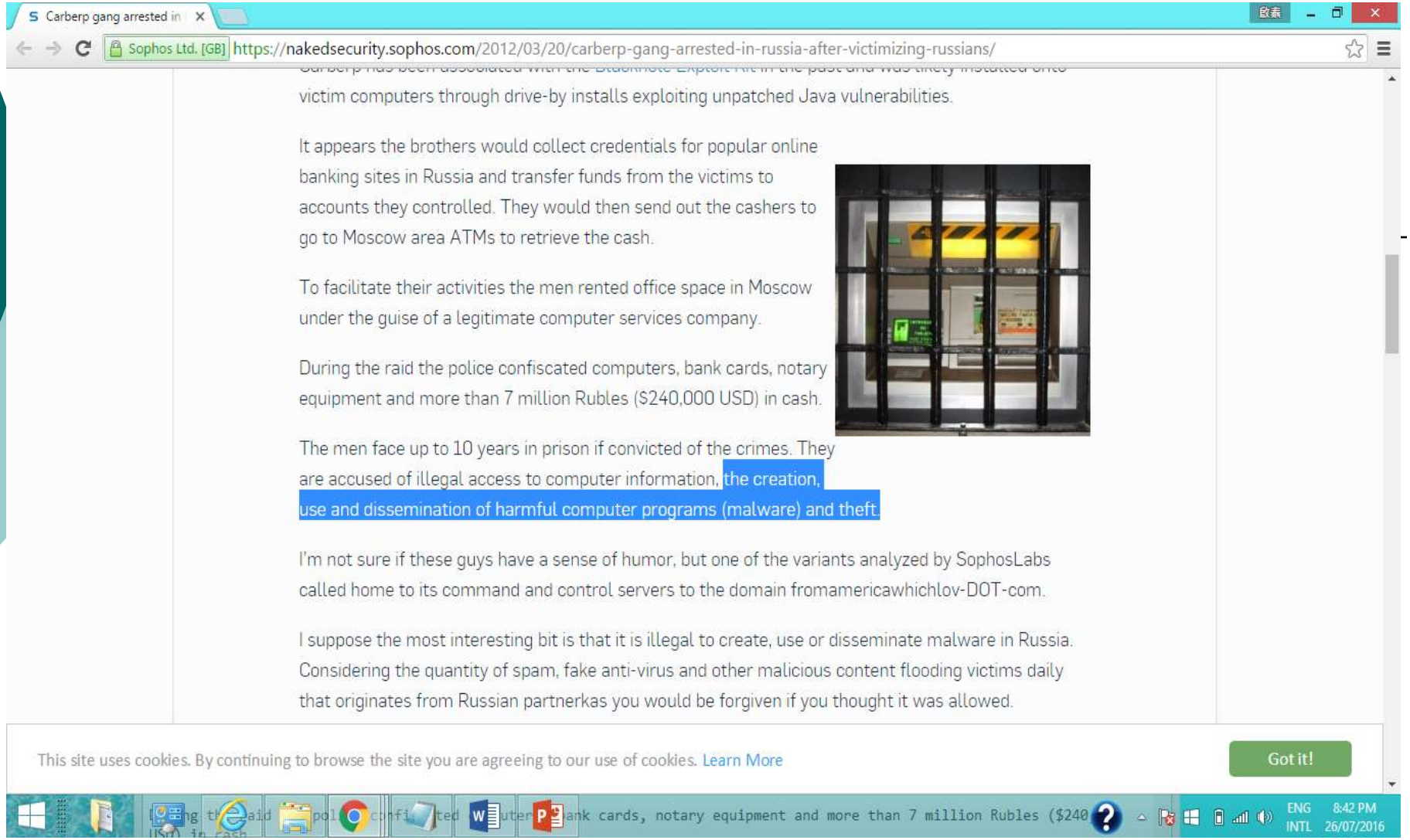
- Cyber black markets for hacking tools or services
- In July 2016, the ATM heist of Taiwan First bank
- Well-known Carberp malware family, which is available for sharing, sale or cooperation on such markets.
- Review organizational cybercrime activities and ATM threats
- Propose an ICT governance framework in online ATM heist management.
- Points out capable people, efficient process, effective technology, and data governance.
- Useful for cybercrime prevention.

The Russian Office of the Interior Ministry and the Federal Security Service (FSB) announced today the arrest of eight suspects connected with the distribution and use of the Carberp malware.



https://nakedsecurity.sophos.com/2012/03/20/carberp-gang-arrested-in-russia-after-victimizing-russians/

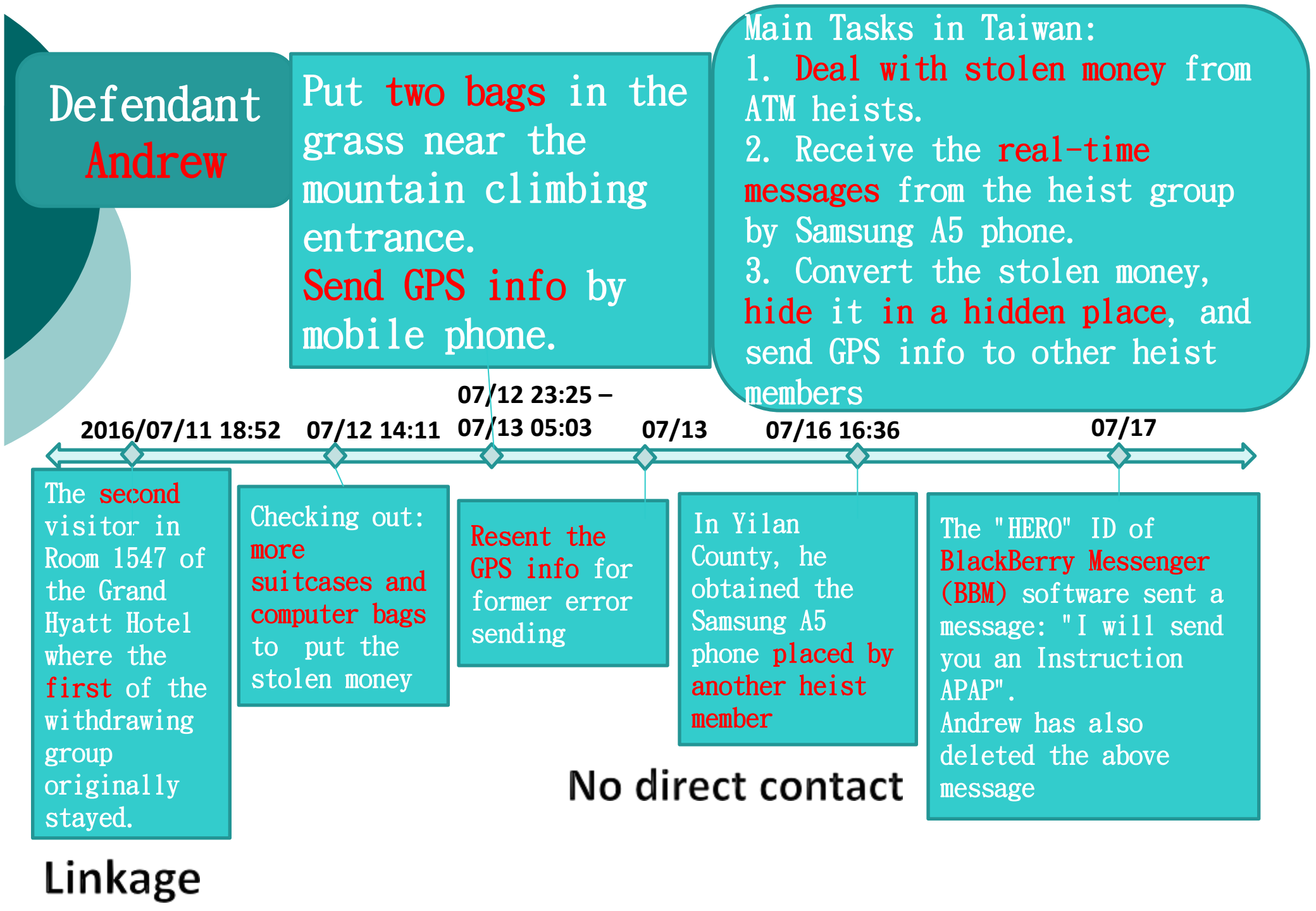
The creation, use and dissemination of harmful computer programs (malware) and theft.



http://krebsonsecurity.com/2014/12/gang-hacked-atms-from-inside-banks/#more-29206

Organizational Cybercrime Activities

Year	Group Name	Actor Type
1993~2001	DrinkOrDie (DoD)	Non-state
1996~1998	The Wonderland Club	
2003~	Anonymous	
2006~2008	Dark Market	
2006~2010	PLA Unit 61398	State
	Shady RAT	
	Aurora	
	GhostNet	
2007~2013	PRISM	
2010	Operation Olympic Games	
	Stuxnet	
2010~2012	Ukrainian ZeuS Group	Non-state


Defendant
Andrew
Put two bags in the grass near the mountain climbing entrance.
Send GPS info by mobile phone.
Main Tasks in Taiwan:
1. Deal with stolen money from ATM heists.
2. Receive the real-time messages from the heist group by Samsung A5 phone.
3. Convert the stolen money, hide it in a hidden place, and send GPS info to other heist members
2016/07/11 18:52
07/12 14:11
07/12 23:25 – 07/13 05:03
07/13
07/16 16:36
07/17
The second visitor in Room 1547 of the Grand Hyatt Hotel where the first of the withdrawing group originally stayed.
Checking out: more suitcases and computer bags to put the stolen money
Resent the GPS info for former error sending
In Yilan County, he obtained the Samsung A5 phone placed by another heist member
The "HERO" ID of BlackBerry Messenger (BBM) software sent a message: "I will send you an Instruction APAP".
Andrew has also deleted the above message
No direct contact
Linkage

Pay the fee and enter the password to take out three suitcases from the locker at Taipei Station

Defendant
Michal

2016/07/10

Send a message to ID "Roma" in the WeChat Messaging software of iPhone 6

07/16 16:54

Take out the second big suitcase

Defendant
Pankov

2016/7/16

09:52

Have a conversation with "A" ID in the Viber cross-platform VoIP IM software application of IPhone 5S

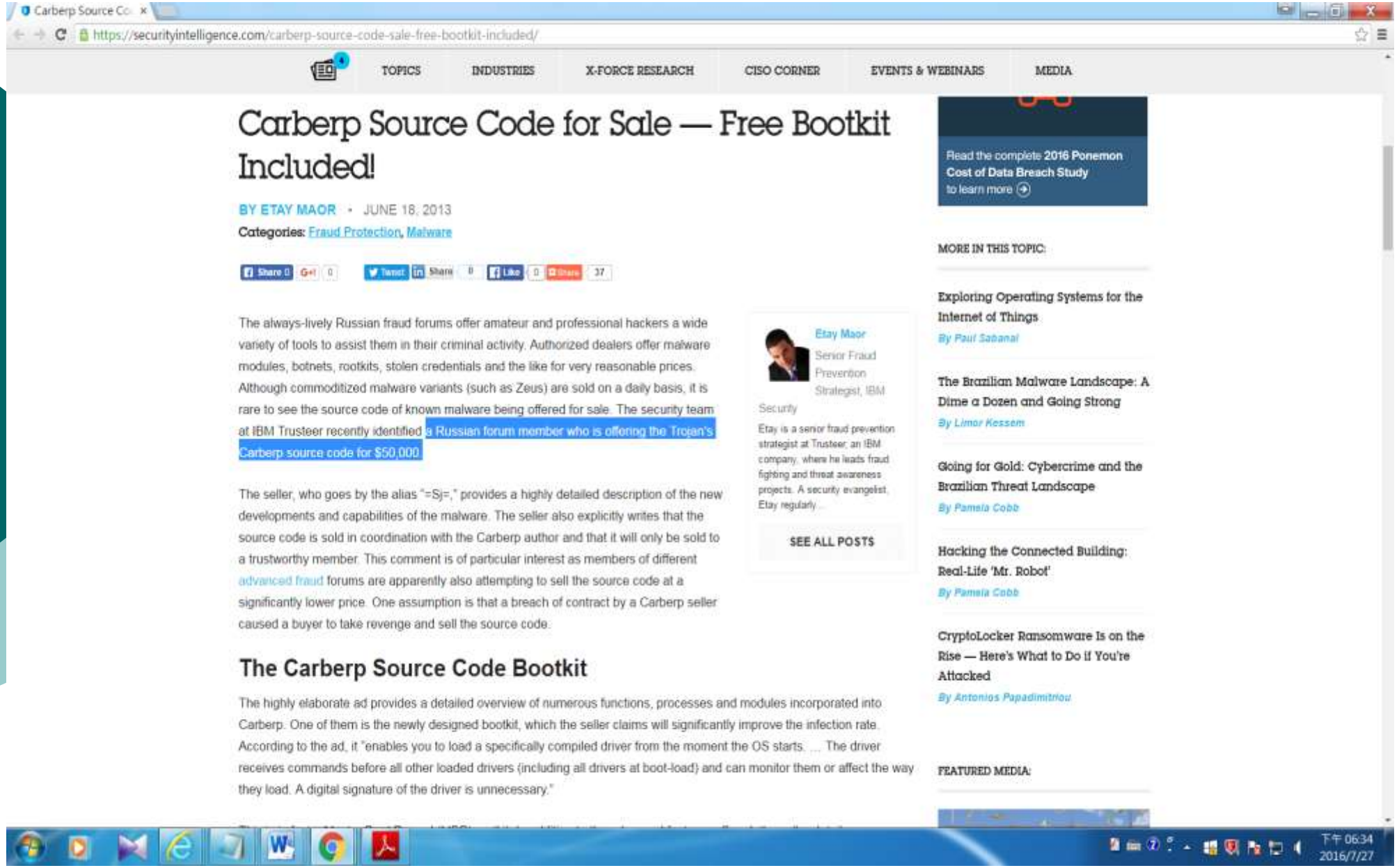
16:41

Take out the first small suitcase

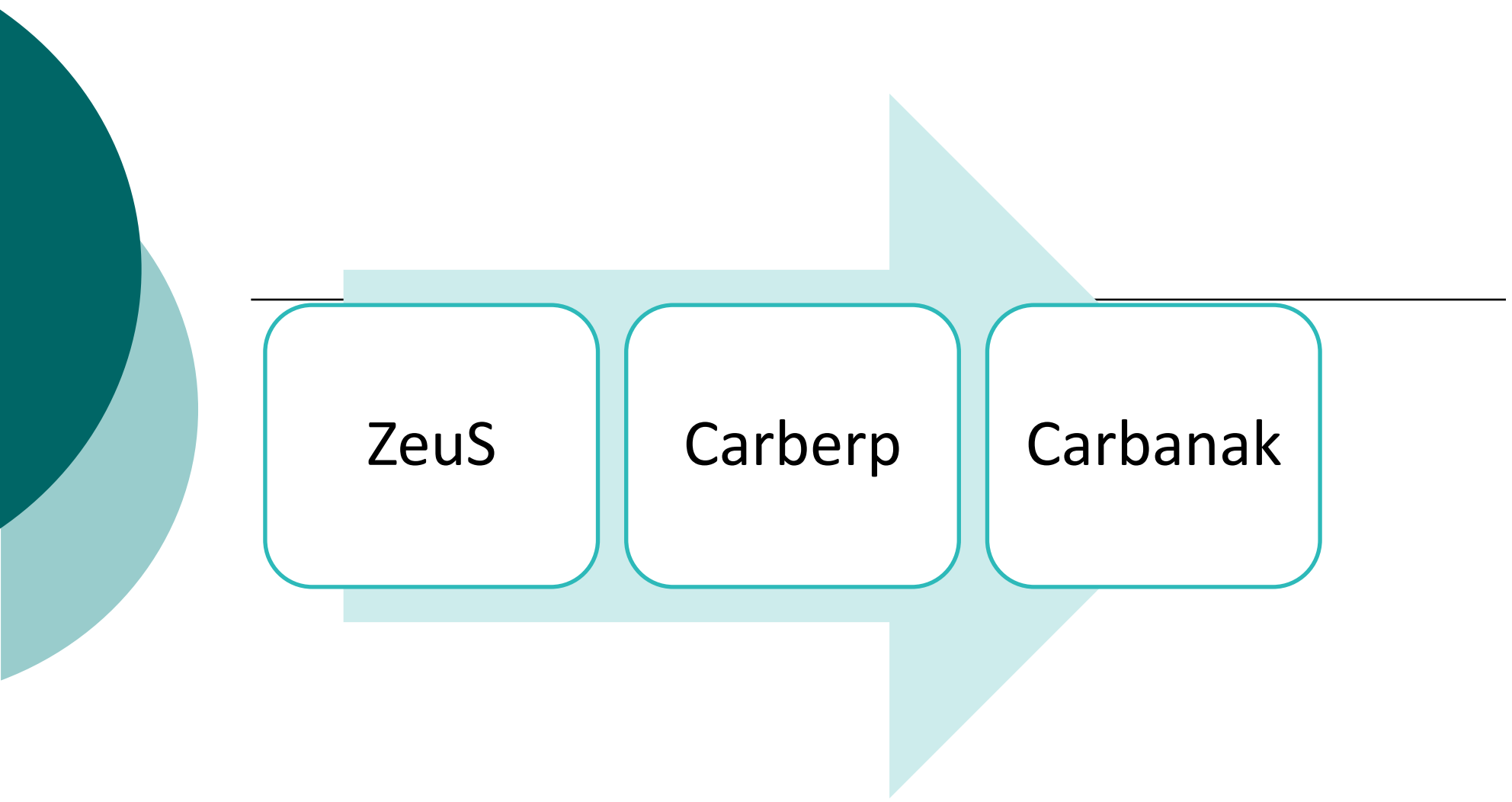
16:50

17:10

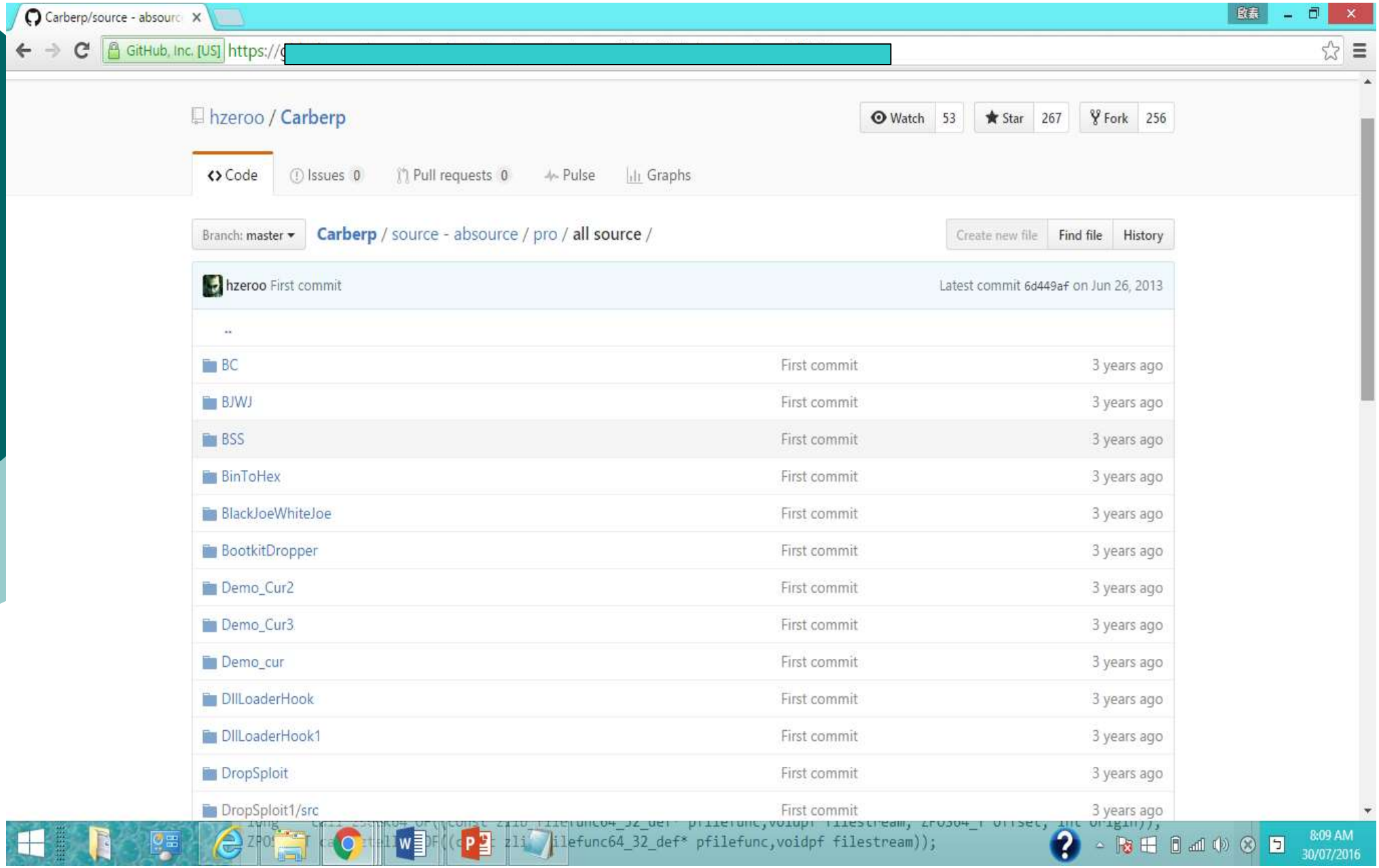
Take out the third big suitcase



https://securityintelligence.com/carberp-source-code-sale-free-bootkit-included/


ZeuS
Carberp
Carbanak

Sharing Malware Source Codes



The Functional Comparison of ATM Malware Family

Malware Family	Carberp	Anunak	Carbanak
Group	Carberp, Pawn Storm or APT28	Anunak hacker group	Carbanak criminal gang
Identified by the Internet security companies	Federal Office for Information Security, BSI (Germany) and Trend Micro (Taiwan).	Group-IB (Russia) and Fox-IT (The Netherlands)	Kaspersky (Russian/UK)
Malware Successor (initially based on)	Zeus, Rovnix, RDPdor, Hodprot, and Origami		Carberp (source code) + Anunak (Wincor ATMs)
Finding Time	2009	December 2014	2015
Victim Location	Russian	Eastern Europe, the U.S.	Russia, the United States, Germany, China and Ukraine

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 USA (More than 24 countries)	Taipei City, New Taipei City, and Taichung in Taiwan
How	Money from	the financial institution itself	Prepaid Debit Accounts	the financial institution itself

Cybercrime threat from Hackers

1) Cybercrime threat

- Exploitable vulnerabilities to computer system
- Increasing expertise of cybercriminals
- Undetected cybercrimes on malware attacks

2) Profiling hackers

- Cross-broader Hackers in Organized Groups
- Black Market for Profit-oriented Hackers
- The Need for Profiling Hackers

ATM Malware Family

- The online banking malware of Carberp program is reported to have impacted hundreds of financial institutions around the world since 2009.
- 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.
- Since 2012 several ATM heists of this type were reportedly carried out in **Russia, Europe and the USA**.
- In 2015, an international organized crime ring had stolen up to US$1 billion from **more than 100 banks in 30 nations.**

Cyber-attack phases and incident response

- Various forms of cybercrime use different malware to achieve specific goals.
- To cope with these threats, LEAs can utilize various security toolkits to collect evidences in cyberspace.

Cyber-attack phases

1) Reconnaissance and Foot printing

Reconnaissance: Gather Big-picture Information

Foot printing: Gather Specific Information

2) Scanning and Enumeration

Scanning

- **Run scanning activities**
- **Attempt to control or infect the computer based on the inferred vulnerability**
- **Run a ping sweep or a network mapper**

Enumeration

- **Connect to a target system**
- **Identify usernames, computer names, network resources, shares, and services.**

Cyber-attack phases

3) Gaining Access	**Hackers can gain access to the system, crack a password, and escalate privileges.**
4) Maintaining Access	**The objective of maintaining access is to ensure hackers can have a long-term access.**
5) Covering Tracks	**Hackers attempt to conceal their trails, manipulate the event logs, and avoid detection by the system administrator or LEAs.**

Digital investigation processes class in ISO/IEC 27043:2015

Processes Class	People	Process/Activities	Technology
Readiness	An organization	Pre-incident investigation/plan and prepare	Cyber-attack phases
Initialization	First responders	Digital investigation/ respond	Live forensics
Acquisitive	Lab managers	Physical investigation/ identify, collect, acquire, and preserve	Dead forensics
Investigative	LEAs	Event reconstruction/ understand, report and close	Digital forensic analysis

Profiling Cybercriminals in Taiwan ATM Heist

SAMPLE CASE: TAIWAN ATM HEIST

Whom are victims?

- ***Target:*** *T*he First Bank's network, The Wincor Nixdorf ATM framework

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.

They use malicious software and defy the bank effort to strengthen the security controls of ATM fleets. This case has demonstrated bank systems lack adequate security measures to stop cybercrimes.

- ***Whom are cybercriminals?***
- ***Offender:*** Cybercriminals were found over many countries.

Three cybercriminals were arrested on July 17, 2016. The 19 escaped cybercriminals have been put on a wanted list, and a total of 22 cybercriminals from six countries were involved.

- ***How did hacker do?***
- ***The Heist*:** The ATM machines simply spited out bills without using ATM cards or touching the ATM.

A **dead drop** is a method of espionage tradecraft used to pass items or information without meeting each other directly. Another method of **live drop** is used when two persons meet to exchange items or information.

Why did this attack happen?

- Organized criminals can rent hackers to conduct attacks or hire middlemen to handle the sale of stolen information.
- The profit attracts hackers by running vulnerable services.
- Cybercriminals try to maximize their financial gain while minimizing their risk.

Behavioral attribute of ATM malware family

Physical Process

- Criminals under arrest
- Shadowy criminal group
- Assistance from other countries' LEAs
- On-Premises to withdraw cash

Virtual Process

- 32-bit Windows ATM platforms
- Through the ATM's pin pad
- No user account required
- Avoiding detection

Exploring Hacker Methodology in Taiwan ATM Heist

Reconnaissance and Footprinting

- Cnginfo.exe and cnginfo_new.exe can read the information inside the ATM.

Scanning or Enumeration

- These activities can be found from the target's firewall log files.
- Auditing logs can be monitored to detect threatened incidents in a timely manner.

Gaining Access

- The hackers initially compromised a vulnerable telephone recording computer used by the targeted bank in order to establish an internal network access.

Exploring Hacker Methodology in Taiwan ATM Heist

Maintaining Access

- They utilized the remote commands to empty the cash-carrying cassettes in the infected ATMs.
- The malware was controlled via the bank's network

Covering Tracks

- Hackers deleted (sdelete.exe) components of the malware employed in the ATM heist.
- Sdelete.exe and batch file cleanup.bat deleted the other programs.

Public-private partnerships

- Technical minds alone cannot solve the issue of prosecuting cybercriminals.
- This must be approached by a team of policing and technical minds.
- 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.

Proposed Strategy on ICT Governance

People

- Commit Cross-Border Cybercrimes
- Need for Global Cooperation

Process

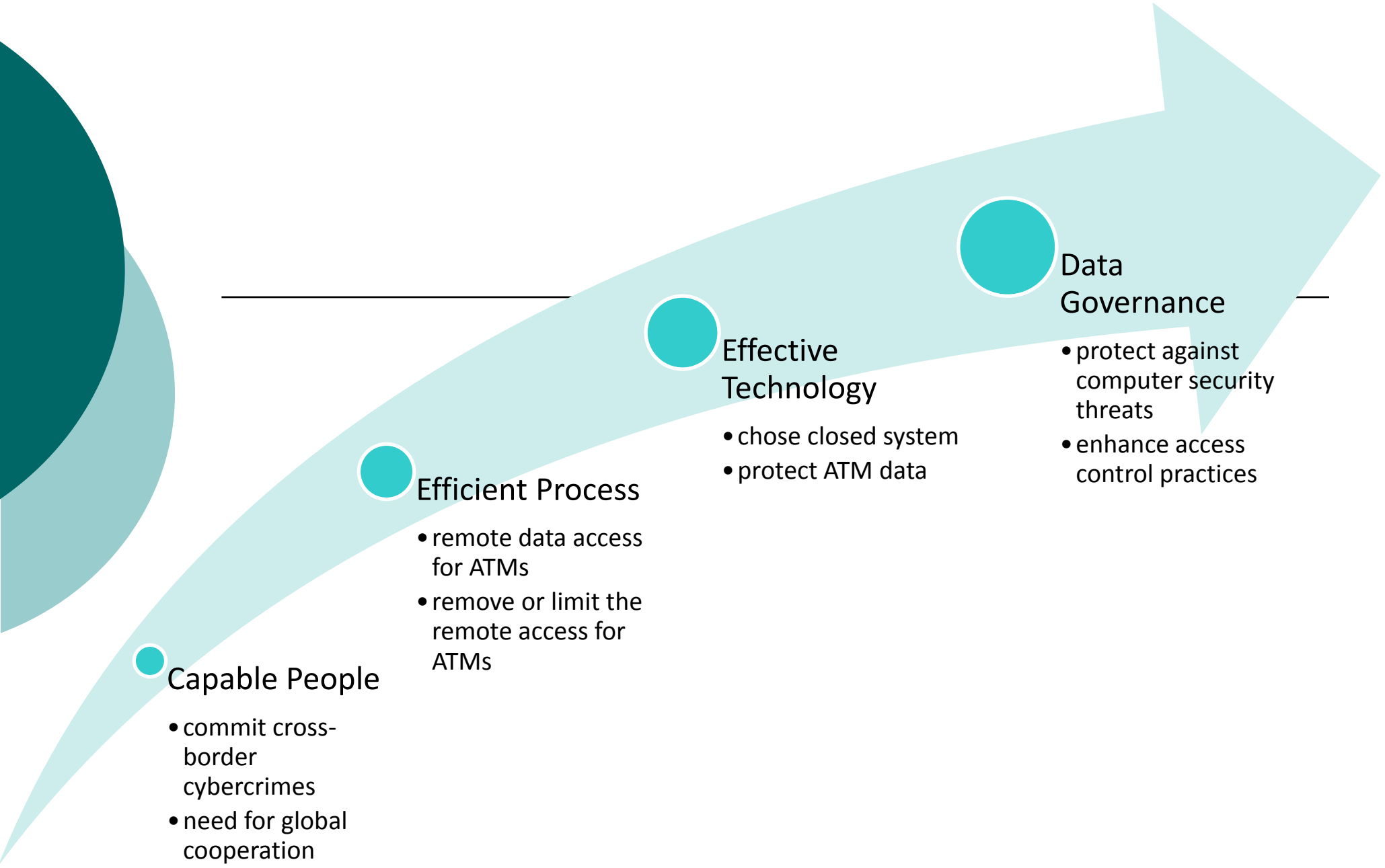
- Limit Remote Access for ATMs
- Limit Convenient Access for ATM Cabinets

Technology

- Chose Closed System
- Protect Internal Information

Governance

- Protect against Computer Security Threats
- Enhance Access Control Practices


Capable People
• commit cross-border cybercrimes
• need for global cooperation
Efficient Process
• remote data access for ATMs
• remove or limit the remote access for ATMs
Effective Technology
• chose closed system
• protect ATM data
Data Governance
• protect against computer security threats
• enhance access control practices

Hacked financial industry in Taiwan

遠東商銀
Far Eastern International Bank

- From January 24th to February 3rd, 2017, 13 firms were victimized in DDoS attacks. The attack lasted about 15 minutes to 1 hour.
- February 7, 2017: The online ordering system of 4 securities companies was damaged in DDoS attacks again. They resumed operation within 30 minutes on average.
- October 2017: Hackers invaded the SWIFT of Far Eastern International Bank (FEIB), implanted malicious programs, and hackers secretly stole up to 60 million US dollars of money abroad

Source: **https://www.ithome.com.tw/news/117386**

HACKED SWIFT Case in Taiwan

- Hackers are familiar with this bank system,
- After invading the internal network, they have deleted 7 anti-virus programs.
- Run a Ransomware to encrypt files on some computers
- Cover the traces of invasion and theft of remittances
- The bank mistakenly thought that it was only implanted with Ransomware.

Malware Characteristics in FEIB, Taiwan

Malware	Detected Name	SHA1
msmpeng.exe	BKDR_KLIPOD.ZTEJ-A	bdb632b27ddb200693c1 b0b80819a7463d4e7a98
splwow32.exe	BKDR_KLIPOD.ZTEJ-B	c7e7dd96fefca77bb1097 aeeefef126d597126bd
FileTokenBroker .dll	TROJ_BINLODR.ZTEJ-A	f891fde8908ae18801d7a 0be1eeab07391c00c1b
bitsran.exe	RANSOM_HERMS.A	b30daf74b25b8615ada1 0cca195270c32e6b343a
RSW72CE.tmp	RANSOM_HERMS.A	d08573c5e825b7beeb96 29d03e0f8ff3cb7d1716

Remote Control IP Address

- **Account:** The hacker obtains the highest-privilege account and connects to a SWIFT server that is not physically isolated.
- The attacker can further control the SWIFT system.
- **Remote Control IP Address: 94.23.148.41 and 167.114.32.112**

Day 1

- On October 3 2017, abnormal network behavior was detected from the **security alerts**.
- A hacker attacked and a **virus** program was implanted. At the time, it was found that only the PC and the Windows server were **affected**.
- The rest of the main transaction systems, such as deposit, remittance, online banking, ATM, and credit cards, are operating normally, and branch services are operating as usual.
- Therefore, the bank initially thought it was just **a simple virus intrusion incident.**

An incident response team

- The bank first set up an incident response team in the information security office.
- The bank also invited a number of security professionals, such as **Trend and Microsoft**, to form a team to check the system to confirm the scope of influence.
- Later, it identified and deleted **viruses and backdoor** programs.
- In particular, it also found viruses that had **not appeared in the past**.

Microsoft's help

- Microsoft originally had a long-term staff at the bank.
- Check whether the Microsoft environment of the bank is abnormal
- Check the system architecture, permissions, user audit management mechanism, and event records for AD services.
- Check for zero-day exploits. However, no such weknesses have been found.

After Day 2 (Holiday)

- On October 5, 2017, the bank found 7 counterfeit transactions when reconciling **after the SWIFT system was repaired.**
- The bank was surprised that the SWIFT bank-to-bank **cross-border transfer system** was attacked by hackers.
- Hackers hacked into the SWIFT system to manipulate transfers, **steal huge money**, and transfer them to different overseas banks in batches.
- **60.104 million US dollars**
  - 57 million US dollars were remitted to **Cambodia**
  - 2.1 million US dollars were transferred to **Sri Lanka**
  - 1 million was remitted to a **U.S.** bank account.

Day 3 (Day 2 is Holiday)

- The bank went to the Criminal Investigation Bureau (CIB) to **report the case**, and asked INTERPOL and the SWIFT Alliance to **assist in the investigation**.
- The hacked computer was also sealed and handed over to the CIB in order to **clarify the hacking methods**.
- At the same time, the bank reported to the Financial Supervisory Commission, Taiwan.
- **Cross-boarder Cooperation:** The Sri Lankan police, based on information provided by the Taiwan CIB, arrested two Sri Lankan men who were trying to withdraw money from a bank in Ceylon.

Analysis for bank SWIFT incidents

1. The **bank's intranet** was intruded by hackers;
2. The hacker also **invaded and mastered** the server of the SWIFT international remittance transaction system;
3. The hacker can **remotely connect** to the SWIFT server through the network;
4. In the case of the hacking of the Central Bank of **Bangladesh** and the hacking of the **Vietnam** International Pioneer Bank, there were signs of **misspellings** in English language.

Improving Information security

1. Application control should be implemented.
2. Integration Check: It is necessary to implement file integration testing and system integration testing.
3. Access Control: All connection control, account control, and privileged account management must be closely controlled.
4. Auditing Log and Record: All aspects of the management are implemented.
5. All security personnel or operators must be sufficiently alerted. If the **warning only appears once**, it must be **tracked down and confirmed**.

New requirements to the SWIFT

1. Domain isolation
2. Network entity isolation
3. Access through the operating room
4. Remote access with two-factor authentication

New requirements to the SWIFT

- **Domain isolation**: Use Microsoft servers with IPsec and Active Directory (Directory Services) to isolate the server from the domain.
- **Network entity isolation**: This is common in the military or important organizations in Taiwan. The intranet users will not connect to the public network during data exchange and transmission.
- To avoid the risk of data leakage, the internal network is a completely closed. When data is exchanged, it requires a **third-party storage medium**, such as a USB flash drive.
- Implement stricter access control measures for each bank's international remittance system.

Today's threats to online banking

- Online banking is popular
- But many people fear that it is insecure
- Wherever money is involved, criminals appear trying to steal it!
- Not only phishing emails with obscured links anymore
- Targeted malware attacks are increasing

Small sacrifice in convenience

- ICT innovations are not only set to bring enormous benefits to the general public, but also bring new technological risks to individuals and businesses.
- The malware is being continuously updated. Old 15-year-old system often opens security holes for hackers.
- A small sacrifice in convenience can be useful to prevent an attack in the ATM's door.
- The ICT governance should be employed by banks to heist ATM money with more barriers.

Summary

- Malware **targeting financial services** exists and increases in number. Why? There is money involved!
- Software running on compromised systems can be targeted and must **protect itself wisely** or it will be rendered useless.
- Most solutions today can solve the technological problem but not **the insider (employee) issues.**
- There are possibilities to protect, so **don't give up the fight!**

中央警察大學
CENTRAL POLICE UNIVERSITY

- **Don't believe everything you are told!**
- **Ask "Where is the EVIDENCE?"**

Dayu Kao (Ph. D.)
Associate Professor
Central Police University, Taiwan
E-mail: camel@mail.cpu.edu.tw

Any comments are appreciated.

Thanks for your listening.