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**

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.