Need Tickets? A Case Study of Bot-enabled Ticket Scalping

Chang-Cheng Lin*†, Hsu-Chun Hsiao†
*Criminal Investigation Bureau, National Policy Agency, Taiwan
†National Taiwan University, Taiwan

***Abstract*—Ticket scalping is considered controversial and even illegal in several countries. With the help of computer program, advanced scalpers can instantly harvest a large quantity of tickets while remaining elusive. This talk aims to provide an overview of the bot-enabled ticket scalping problem from technical, business, and law perspectives. This talk will also share an investigation conducted by Taiwan Criminal Investigation Bureau (CIB) in January 2017, including the mechanism and challenges encountered during the investigation. We hope this talk can stimulate collaboration and innovation in fighting bot-enabled ticket scalping worldwide.**

1. Introduction

As more and more events are selling tickets online, ticket scalping (or ticket resale) is easier than ever: A reseller can gain unfair advantages by using computer program to purchase a large number of tickets within seconds, whereas a normal customer often finds it difficult to secure even one ticket for popular events (e.g., concerts, games, and transportation in holiday seasons). Thrived on the customers' desire, such unauthorized resellers can easily earn huge profits after reselling the tickets on non-official websites.

From a law perspective, several government authorities have begun to regulate bot-enabled ticket scalping. For example, the U.S. signed a federal ban in December 2016 to restrict the usage of computer software for online ticket purchase. This federal ban aims to ensure fairness and prevent resellers from obtaining a large amount of tickets before normal customers. On the contrary, when the Criminal Investigation Bureau (CIB) solved the first ticket scalping case in Taiwan in January 2017, there was no legal precedence for the prosecution of ticket scalping. The law enforcement agency (LEA) had to look for relevant laws and regulations as we will explain later.

Talk structure. The proposed talk structure is as follows:

- We first introduce the ticket scalping problem, and summarize several high-profile incidents and regulations in different countries.
- We then present a case study regarding a recent ticket scalping case solved by Taiwan Criminal Investigation Bureau, with an emphasis on the mechanism we developed to systematically detect, analyze, and investigate ticket scalping.
- We conclude this talk with suggestions to the ticket sellers and the law enforcement, and how the community can work together to mitigate ticket scalping.

We highlight the main ideas in the rest of the proposal.

2. Detecting Bot-enabled Ticket Scalping: Proposed Mechanism and A Case Study

The second part of the talk will introduce a ticket scalping case conducted in December 2016 and solved by CIB in January 2017. At a high level, the investigation of ticket scalping can be divided into five steps: (1) Definition of a normal ticket ordering behavior, (2) Statistical Analysis, (3) Human-Bot Detection, (4) Pattern Matching, and (5) Cyber-Crime Scene Investigation.

In this case, after the victim filed a report about suspicious web activities, the CIB analyzed the web logs of the victim website and discovered many connections established right before the start time of ticket selling. Using pattern matching and statistical analysis on the web logs, the CIB network forensic analysts were able to identify several IP addresses and member accounts that might belong to the ticket bots. After getting the warrant, the CIB investigated the suspect's computer and found automatic ticket scalping tools on the suspect's computer. These tools are written by the suspect and each of which is tailored for the ticket ordering flow of a target website. The suspects sold those tickets at a higher price than the original one to earn money.

Ticket ordering behavior. Since each website's implementation may differ, it is crucial to define the normal ticket ordering flow before we can identify the abnormal ones.

Hence, we discussed with the website administrator to understand the internal state transition, which is illustrated in Figure 1: The customer browses the web page to choose the show number, then the customer sends the number of tickets he/she wants to order to the website. After the website responds to the customer's browser that the tickets are granted, the customer needs decide the payment method (ATM or credit card) and then will be redirected to the final payment confirmation page.

Statistical analysis. After identifying the ticket ordering flow, we analyzed the number of connections around the ticket selling time (14:30:00), as shown in Figure 2a (10s interval). The number of connections started to increase about three minutes before (14:26:3*) and become saturated

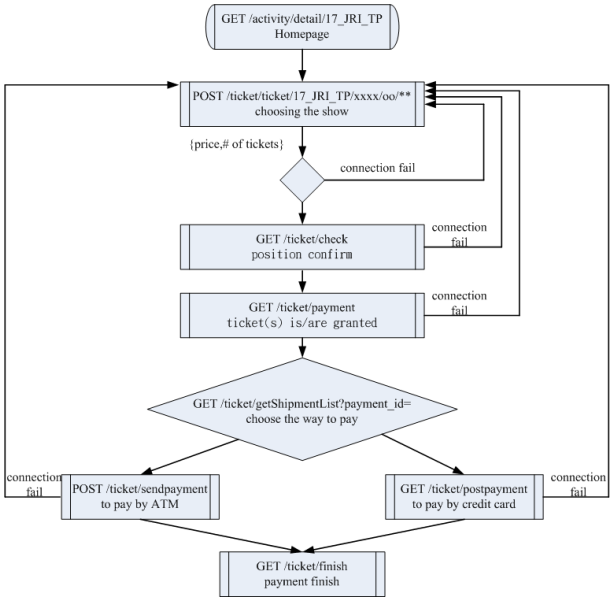


Figure 1: Ticket ordering flow of the victim website

around 14:29:3*. When the ticket sell started, the number dropped to 583 from 4,942. There is another burst at 14:30:1*, which we think it represents the manual connection re-trial after timeout by the the human customers.

Bot detection. The next challenge is to differentiate humans from bots among the burst of connections right before ticket selling. The key observation here is that a bot often has a much shorter transaction time than a normal human user since it takes time for a human user to type, process, and response to the server. Although in general bots could be designed to mimic human behaviors (e.g., introducing delays), there is little incentive for a ticket scalping bot to pause between actions because it will also decrease the chance of getting tickets. The CIB analysts computed the average transaction time of known normal users (provided by the victim) and used it as a threshold to identify bots.

Pattern matching. After obtaining the baseline (e.g., the average transaction time of normal users or the number of connection attempts per second) for a particular victim site, we can identify IP addresses that are likely associated with the criminals. For example, the CIB analysts used Log Parser Lizard [1] to compute the number of successful transactions per member account and check whether these member accounts can complete a transaction in a short time. By doing this, the analysts found several suspicious accounts with similar receiver names and corresponding physical addresses, which were used to receive the physical tickets from express delivery. Even though these receivers may not be the actual suspect, they must be associated with the suspect in real life. Although using physical tickets (instead of digital ones) seems inconvenient to users, in this case it helps track down the suspect in the real world.

Cyber-crime scene investigation. To find conclusive evidence, the analysts examined the suspect's computer for bot programs, which may be source codes, config files and compiled executables. Several automated programs written by the suspect himself were found. A snippet of the source code is shown in Figure 2c.

3. Challenges and Discussion

The last part of the talk will discuss challenges in catching ticket scalpers.

For example, different ticket selling sites may have different ticket ordering flows and log formats. How can we standardize the incidence response procedure and reduce manual efforts in investigating individual cases? This is crucial for achieving timely investigation and preventing the tickets from being resold. Also, accurately distinguishing normal users from resellers remains challenging, because fanatic users are always developing tricks (e.g., leveraging browser auto-fill features, writing bot-like scripts, etc.) to "beat" the ticket selling sites.

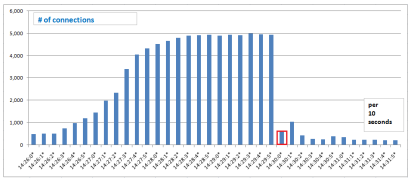
In addition to technical challenges, the lack of proper laws and regulations also hinders the investigation. Since the case described earlier was the first solved case in Taiwan, it was unclear which law CIB could apply to prosecute ticket scalping. In the end, the Article §360 was quoted: The Articles §358 362 of Criminal Law in Taiwan focuses on cyber crime, and particularly, the Article §360 focuses on hacking behaviors that interfere with someone's computer operations. In the ticket scalping case, since the scalpers attempt to harvest an excessive number of tickets from the official ticket selling website in a short time, the website was under a DDoS attack and could not serve normal users.

To defend against bot-enabled ticket scalping, ticket selling sites can adopt common techniques such as CAPTCHAs, WAF policies, and real-name systems. In Taiwan, several major events (e.g., popular music concerts and train tickets to remote areas) began to request for the user's real name during online purchase since 2016. The name is printed on the ticket and will be checked against the user's ID at gates. However, to circumvent real-name systems, scalpers have developed a new business model, in which they ask for the buyers' name, birthday, phone number and national ID in advance and purchase tickets (possibly using bots) on behalf of the user. It remains unclear how to detect such a new ticket scalping model and whether it is considered illegal.

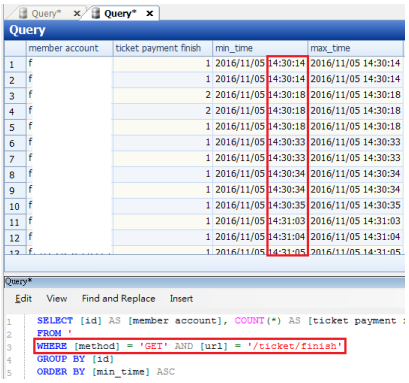
4. Expected Contribution

The objective of this talk is to shed light on analysis and investigation into ticket scalping by sharing our experience and methodology for tackling ticket scalping in Taiwan.

Since ticket scalping is a relatively new type of cybercrime, and only few of the ticket-scalping cases have been solved internationally, we hope this presentation can contribute more insights to the ever growing problem. We envision the methodology we developed can serve as a working reference for other LEAs around the world. We also hope to receive feedback and collect more real-world cases from the participants, thereby collaboratively improving the methodology.



(a) Number of connections



(b) Anomaly Patterns

(c) Ticket scalping tool

Figure 2: Case study investigation

References

[1] "Log Parser," https://www.microsoft.com/en-us/download/details.aspx?id=24659.