USB Baiting

Project Proposal

Daan Wagenaar, Dimitar Pavlov, Yannick Scheelen

Universiteit van Amsterdam

1 General information

Research Members:

Daan Wagenaar	Yannick Scheelen	Dimitar Pavlov
daan.wagenaar@os3.nl	yannick.scheelen@os3.nl	dimitar.pavlov@os3.nl

2 Background Information

The so-called "USB baiting" is a social engineering technique that aims to provide access to a target computer or computer network. This is accomplished by planting USB sticks with malicious contents at places, where these USB sticks are likely to be found by the users of the targeted system/network. The attack relies on the assumption that users are curious about the contents of a found USB stick and are likely to simply plug the USB stick into their computers. Once the USB stick has found its way to the target system/network, the payload (either backdoor software, or information gathering software) can be activated and the goal - accomplished.

The technique of USB baiting is a common one, being used both by actual attackers to penetrate a system or network, and by penetration testing professionals to asses the likelihood of users plugging-in an unknown USB stick into their computers. And thereby exposing themselves and the company they work for to unknown risks to the infrastructure and possible confidential information.

Although this is a common social engineering technique, there is little research data available on the topic. Since this technique has been studied mostly by penetration testing companies to assess their customer's security policies, it is unlikely that any research conclusions would have been published, because of confidentiality issues.

3 Project Description

3.1 Research Questions

We want to analyze the tendency of users to plugin a foreign USB drive and investigate the effectiveness of possible USB attack strategies for malicious code execution.

- What is the tendency and reasoning for users to plugin a foreign USB drive?
  - Do different drop-off environments influence the infection rate?
- Which possible USB attack strategies are the most effective for successful malicious code execution?

3.2 Description

By means of USB baiting we want to gain insight into the ratio of Windows users that are susceptible to social engineering attacks of this type.

Also, by planting USB drives at several locations, our research will show whether different drop-off locations influence the success and overall infection rate of certain attack vectors.

Equipping the USB drives with more than one attack vector, will increase the potential infection factor and at the same time allows us to gain insight in the most successful attack vectors.

A questionnaire allows for further investigation into the reasoning why users plugged-in the USB drives, why they opened different content and whether they are now more aware of the dangers of plugging in foreign USB drives.

Another point of interest is to see whether different attack vectors are more successful on different Windows versions.

3.3 Approach

This project can be divided into five phases. Each of these phases entail a certain aspect, from the beginning until the end, of the project.

1. Preparation phase
2. Drop-off phase

3. Infection phase
4. Callback phase
5. Processing phase

During the preparation phase we will prepare the required contents for each attack vector, our backend systems for the callbacks and perform testing to make sure the attack vectors work as they should. The actual preparation of the USB drives will also be done during this phase. Most of the time spent in this project will be during this phase as it entails designing, creating and testing all of the technical aspects mentioned earlier.

In the drop-off phase we will scatter the specially crafted USB drives around different locations. We will select a number of computer rich drop-off areas that are in use by many people. For example, the library or the computer labs. Per selected area, a small set of USB drives will be dropped-off as to not flood the area and potentially make people suspicious.

The infection phase is initiated as soon as one of the scattered USB drives is picked-up. During this phase, some USB drives will be plugged into potentially vulnerable computer systems and possibly one of the attack vectors will result into infection.

Once infection has taken place, the callback phase is started. During this phase, successful attack vectors will perform a callback to our backend systems providing us with information about the users and infected systems. The infection phase also entails the notifying of the user that his computer system is vulnerable as well as presenting the questionnaire and the dangers of USB baiting to the user.

The last phase, the processing phase, will consist out of processing and formatting the gathered data and results. Furthermore it includes the creation of the project report explaining and detailing the found results and made conclusions.

3.4 Setup

Different technical aspects come into play during this project. Each aspect requiring certain designs and implementations. This section is used to give a brief overview of these technical aspects and the choices made regarding the implementation of these aspects.

Attack vectors
Since we will be targeting Windows based computer systems, we will select attack vectors that are known to potentially work on these systems. Each attack vector, if successful, will result in a callback to our backend systems and a notification, letting the user know what has happened.

- Windows autorun
- Windows shortcut bug
- Malicious PDF files
- Plain executables
- URL shortcuts

The executable will be custom made and will only contain a possible user notification and a callback to our systems, no code that alters the system in any way will be present. This same executable will also be used in the malicious PDF files as well as in the autorun mechanism and the shortcut bug.

If we find during testing that one or more of the selected attack vectors are not as effective as expected, e.g. most virus scanners detect them, we might not use them. On this same note, we might also introduce other attack vectors previously not deemed usable.

USB drives
Optimally, 100 USB drives will be provided with multiple instances of the previous mentioned attack vectors.

The exterior of each USB drive will not give any clues about its size or contents that could negatively influence a persons decision to pick up the USB drive.

The file and directory naming as well as the file and directory structure on the USB drive itself, will be designed in such a way that it gives the impression that the USB drive belongs to an administrative worker.

Callback
For the callback mechanism HTTP will be used. We make use of HTTP since most computers behind NAT or Firewall devices can still access arbitrary servers on the web and thus send the needed information.

Each USB drive and attack vector will be provided with their own unique ID which allows us to identify which USB drive was plugged-in and which attack vector resulted in a successful infection.

Additional information might also be gathered and transmitted to our backends. This information is limited to privacy insensitive data – all obtained information will consist only of OS patch levels and user privileges.

Backends
The backend systems will consist of a web server, a database and a PHP website. The latter being able to actually receive, process and store the information gathered from the callbacks as well as present the questionnaire to the visitors.

4 Related Work

One of the first published works on social engineering was the paper [1] "Re-Floating the Titanic: Dealing with Social Engineering Attacks", written by David Harley. It introduced the first ideas of using social engineering to penetrate an information system. In 2002, Kevin Mitnick released his first work [2]"The Art Of Deception" which covers the art of social engineering. The first relevant technical published work on social engineering was also created by Kevin Mitnick and William Simon, in [3] "The Art Of Intrusion". It explains the initial idea of using social engineering to penetrate the security of information systems. It does not, however, feature the use of infected USB drives to do this.

In 2006, the people of Darkreading.com launched the first results of using USB baiting to penetrate the security of a credit union. In their article [4] "Social Engineering, the USB Way", they report 15/20 USB sticks being plugged in and penetrated the computer's security. They used a self-written Trojan Horse disguised as an image in order to get access to the system.

In 2010, the Idaho National Laboratory published studies of in-house testing on USB baiting. A [5] primary study found that 20% of employees who picked up a drive plugged them into work computers, 22% of employees clicked on a URL in the phishing email; and 40% of employees provided passwords to the IT support impostor.

As of today, there are no published papers with conclusive results nor are there reports of studies where different attack approaches on a single USB stick are used in order to penetrate the security of a system.

5 Planning

Our planning will be directly linked to the different phases in our project.

- **Preparation phase**: We start the 17th of November with the creation of each attack vector and our backend systems for the callbacks. The USB sticks will be ordered the 18th of November the latest. Initial work on the final report paper will start here, too. We expect to get the USB sticks before the 25th of November. By then, all the code has to be written so we can start to deploy our codes on all the USB sticks. For testing of the code and our backend system on the USB sticks we estimate that 10 days is sufficient, just in time for the drop-off phase.
  - D. Wagenaar: Create the 'malicious' PDF files; Prepare the backend systems
  - Y. Scheelen: Buying the USB drives; Create the Autorun system
  - D. Pavlov: Create the 'malicious' executable
  - Group Work: Create the PHP website; Prepare the USB drives
- **Drop-off phase**: The 6th of December, we want to drop-off our USB drives.
  - Group Work: Drop off the USB drives at specific locations
- **Infection & Callback phase**: We hope to get swift results; ie. on the same day as the sticks drop-off or at least in the following one or two days. Since our code will automatically send us the results, the Infection and Callback phase will happen simultaneously.

  - Group Work: Monitor the incoming transmissions.

- **Processing phase**: By the 12th of December we hope to get all the results we need. This leaves us two weeks to analyze all the data and finish up the report.
  - Group Work: Analyze and process the results and prepare the final report and presentation.

6 Funding

Based on the approach of [5], and on the fact that our research is exploring five different mechanisms for infecting target computers, five attack vectors, we concluded that for this project to produce the best results, with regards to its scope, the minimum needed number of USB sticks is 100. This many USB sticks will allow for accurate statistical results, as well as give freedom for exploring different attack vectors.

The best current price quote for 100 USB sticks with a capacity of 128MB is 3.50 euro per USB stick. The total needed amount of funding at this price, for this many USB sticks is 350 euro.

However, if the amount of funding available to this project is less than 350 euro, then the goals of this project are still achievable but the relevance of the outcome of the project may be less than optimal.

References

1. Harley, David. 1998 Re-Floating the Titanic: Dealing with Social Engineering Attacks
2. Mitnick, K., Simin, W., and Wozniak, S. (2002). The Art Of Deception. Indianapolis, IN: Wiley Publishing
3. Mitnick, K., and Simon, W. (2005). The Art Of Intrusion. Indianapolis, IN: Wiley Publishing
4. http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1
5. http://www.computerworld.com/s/article/9218214/Government_tests_show_security_s_people_problem