MOBEY FORUM
Mobile Financial Services

Zeus in the Mobile:
Considerations for using SMS as two-factor authentication in online banking

Mobey Forum

MOBEY FORUM
Mobile Financial Services

INDEX

TABLES AND FIGURES LIST

REFERENCES

The following documents have been used as references in the preparation of this document:

Code	Document
RD1	2010 Online Banking Security Survey: Zeus-Like Malware Rapidly Outpaces All Other Online Banking Threats
RD2	Zeus Trojan Horse (http://en.wikipedia.org/wiki/Zeus_(trojan_horse))
RD3	Zeus In The Mobile (Zitmo): Online Banking's Two Factor Authentication Defeated (http://blog.fortinet.com/zeus-in-the-mobile-zitmo-online-bankings-two-factor-authentication-defeated/)
RD4	Zitmo Follow Up: From Spyware to Malware (http://blog.fortinet.com/zitmo-follow-up-from-spyware-to-malware/)
RD5	Zeus Goes Mobile - Targets Online Banking Two Factor Authentication (http://www.securityweek.com/zeus-goes-mobile-targets-online-banking-two-factor-authentication)

1. INTRODUCTION

1.1. PURPOSE

The purpose of this document is to describe the new mobile variant of the Zeus Trojan, known as the Zitmo, and its implications for online mobile banking security, with particular emphasis on how it can disrupt the use of SMS as second factor authentication for online financial transactions. This document will focus on defining Zitmo and how it works, with a view to opening discussion about this threat to mobile.

The new mobile form of the Zeus Trojan affects smartphones where malware finds a good field for infection. With increasing smartphone penetration, we can expect to see a growing number of attacks by Zeus and other kinds of malware.

The limited scope of this document does not permit a detailed analysis of the full spectrum of possible solutions for fighting this type of malware. However, Mobey Forum's Security Task Force is working towards a future document in which solutions could be developed in depth.

2. ONLINE BANKING THREATS AND THE ALMIGHTY ZEUS

Malware targeting financial institutions is becoming increasingly widespread. Likewise, malware coders are rapidly improving their offerings, making them ever more ingenious and effective.

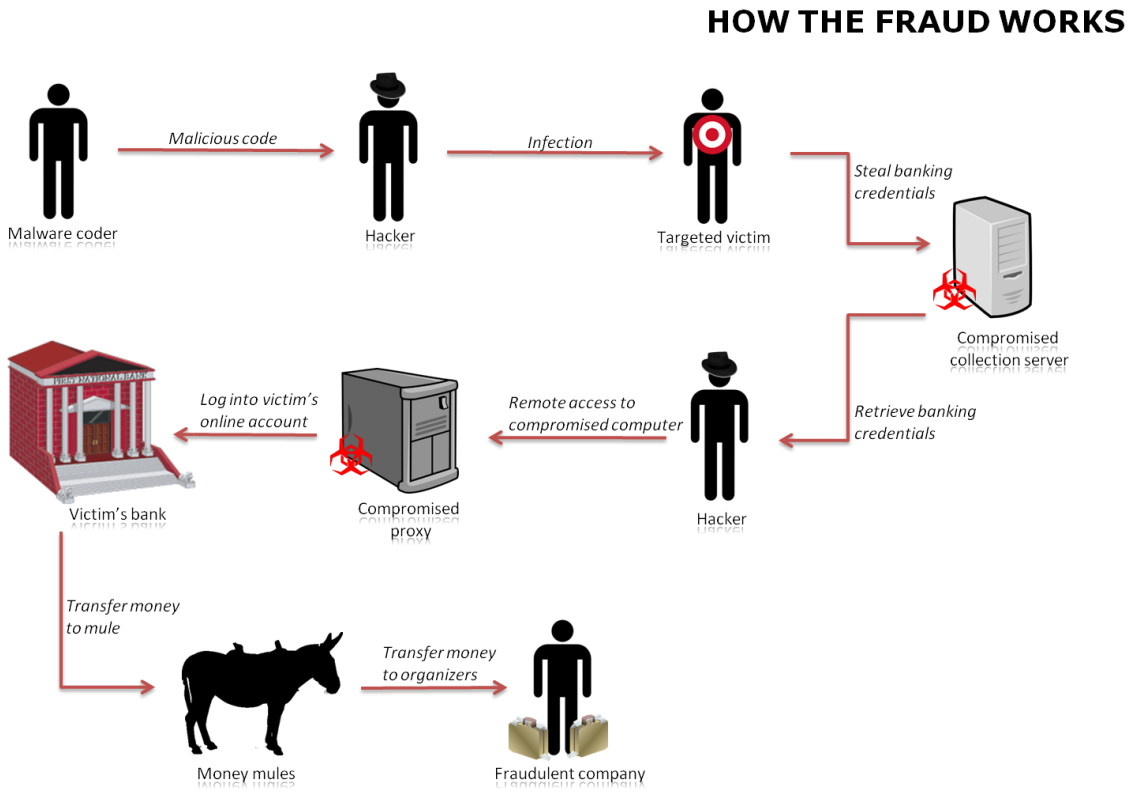

Figure 1 - How the fraud works (source: *www.wikipedia.org*)

One of the best known banking Trojans is the Zeus Trojan, also known as Zbot. Zeus is a Trojan specialized in stealing the credentials used to access online banking accounts. Thanks to its ease of use, the Zeus crimeware kit has become the most popular banking malware. This kit can be obtained in the underground market at a reasonable price, and its use requires almost no advanced programming skills.

The Zeus kit is composed of two parts:

- The bots administration server by means of a C&C control panel,
- The tools needed to create the Trojan binaries together with their encrypted configuration file.

These binaries are distributed and installed in the victim machines by making use of several techniques. Social engineering, such as e-mails purportedly sent by their bank or offering software updates, is used to trick the targeted victim into installing the malicious software.

The Zeus binary is linked to a configuration file which defines the Trojan's functionality as well as the target entities/sites. The configuration file includes the different techniques that Zeus can use in order to steal the victim's information:

- **HTML injection**: When the victim accesses his online bank account, the Trojan overlaps a window requesting extra information or security codes.
- **Web redirects**: When the Trojan detects that a URL is being accessed, it redirects the browser to a previously configured malicious URL that looks practically identical as the original page.
- **Virtual keyboard capture**: The Trojan can be configured to take a screenshot every time that the victim uses the mouse in a certain website. By using this technique, additional security measures such as virtual keyboards can be defeated.

3. ZEUS GOES MOBILE

Since the Trojan was first identified in 2007, different versions of the malware have been developed, with each new version either providing new functionalities or improving the encryption of its associated files to make it more difficult to ascertain its behavior and capabilities.

One of the latest variants of the Zeus Trojan (first reported on September 2010) has a new approach: Instead of focusing on simply infecting the victim's PC, it also infects the victim's mobile phone in order to defeat the SMS-based two-factor authentication that banks frequently use to confirm electronic transfers of funds. This variant has been called **ZITMO** (***Zeus in the Mobile***).

The following diagram demonstrates the flow of events once a user's PC has been infected with a Zeus sample, showing how the infection is spread to the mobile device and how SMS sent from the bank are intercepted.

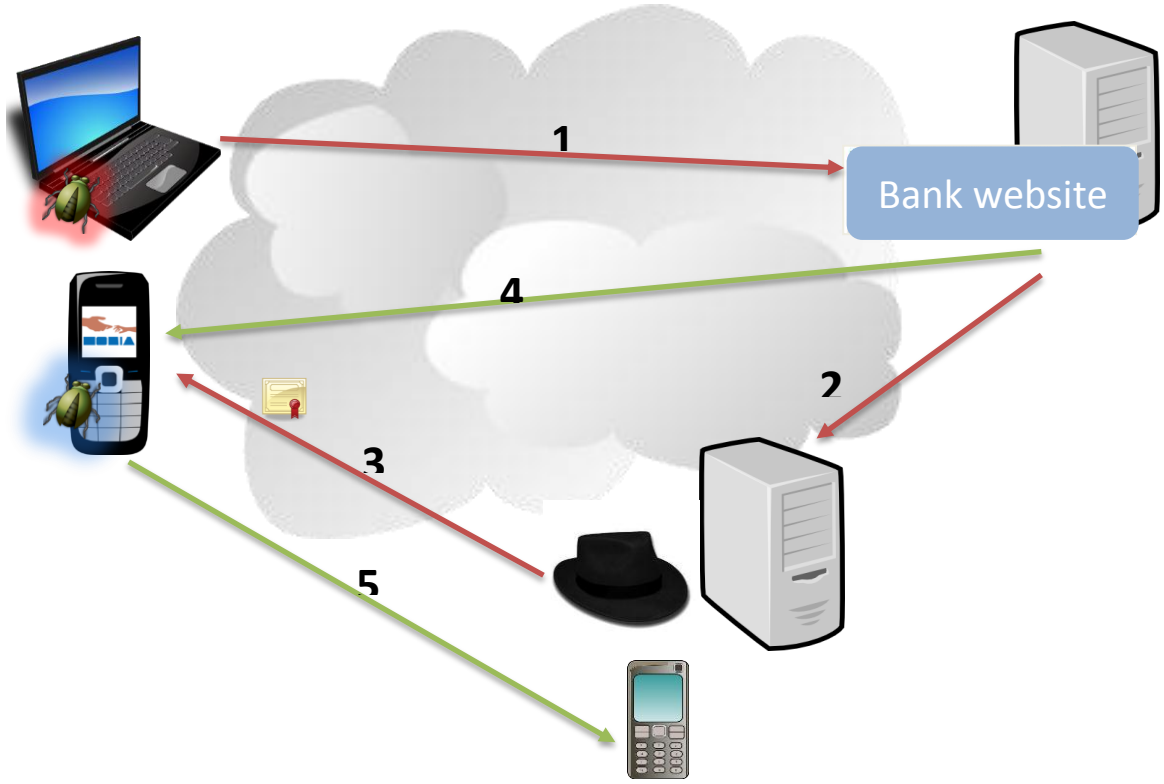

Figure 2 - Zitmo: Flow of events

3.1. DESCRIPTION

1. The victim's PC is infected by a Zeus sample. The user accesses his bank's website (which is one of the Trojan's targets). Zeus overlaps a frame/window over the browser requesting the following data:
    a. User PIN, password, and security codes

Figure 3 - Capturing Security Codes

    b. Mobile phone model and phone number

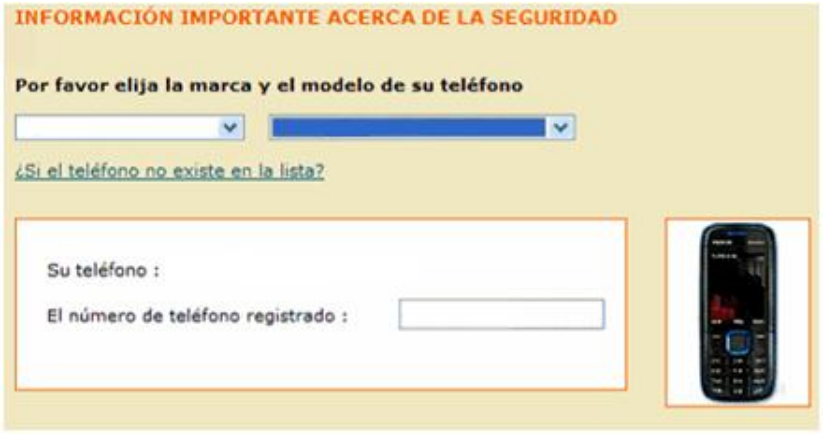

Figure 4 - Capturing Phone Model and Number (source: *www.securityweek.com*)

2. The captured data is sent to the malicious server.

3. With this information, an SMS can be sent to the victim's mobile phone with a link to a security update which is in fact the malicious software written for that mobile platform *(Symbian applications → **.sis** and Blackberry applications → **.jad** have been observed)*. Once the user clicks on the link, the malware is installed in the mobile device. The user will not notice anything strange as the package being installed is correctly signed and appears to be a security update.

Figure 5 - Zitmo installation

4. Once infected, the mobile device will respond to a series of SMS commands that can be used to remotely configure the device in order to intercept incoming SMS and pass them to the attacker. Therefore, the attacker will be able to initiate electronic transfers of funds with the information obtained in Step 1. The bank will then send a confirmation SMS to the victim's mobile phone, where it will be hidden to the user.

Command	Description
SET ADMIN	Change the C&C phone number
ADD SENDER	Set the phone number to be spied on
REM SENDER	Remove the phone number to be spied on
ON/OFF	Turn the spy engine ON or OFF respectively

5. The SMS coming from the bank will be forwarded to the attacker's mobile phone. The attacker will then be able to confirm the transfer without any problems.

3.2. FIGHTING AGAINST THE THREAT

How can banks fight the Zitmo threat?

Although Zitmo is not yet frequently found 'in the wild,' so to speak, it is clear that this Zeus variant is very dangerous thanks to its capacity to defeat the SMS-based two-factor authentication used by banks to secure electronic transactions. Attackers have to make use of social engineering to mislead the user to thinking that he is installing licit software, which is difficult to prevent. However, a solution could lie in the creation of a mechanism within the mobile or online banking environment with the ability to prevent the theft of credentials.

It has been demonstrated that regular out-of-band authentication via SMS is not robust enough to prevent cybercriminals from intercepting communications and stealing the user's credentials. To enhance security, the concept of multi-factor authentication should be developed further, for instance by combining different authentication techniques for a more comprehensive security solution.

The aim of this document is not to develop in depth the whole range of solutions to this threat, but to open the floor for discussion and enable the elaboration of a separate document where solution providers and other intersecting third parties could collaborate on generating new solution suggestions.