Introduction to Trojan.Zbot

Coming from the Trojan Family

Systems Affected: mainly Windows systems

Part 1: Description

Trojan.Zbot, also called Zeus, is a Trojan horse that attempts to steal confidential information from a compromised computer.

It may also download configuration files and updates from the Internet. The Trojan is created using a Trojan-building toolkit.

Part 2: Infection

The Trojan.Zbot allows an attacker to have a high degree of control over the functionality of the final executable file that is distributed to targeted computers. The user may receive an email message purporting to be from organizations such as the FDIC, IRS, MySpace, Facebook, or Microsoft.

The message body warns the user of a problem with their financial information, online account, or software, and suggests they visit a link provided in the email.

The computer will be compromised if the user visits the link, if the computer is not protected.

Part 3: Functionality

<u>Multiple methods to gather confidential information</u>

This Trojan has primarily been designed to steal confidential information from the computers it compromises. It specifically targets system information, online credentials, and banking details, but can be customized to gather any sort of information. This is done by tailoring configuration files that are compiled into the Trojan installer by the attacker. These can later be updated to target other information, if the attacker so wishes.

The Trojan.Zbot's most effective method for gathering information is by monitoring Web sites included in the configuration file, often by intercepting the legitimate Web pages and inserting extra fields. It contacts a command-and-control (C&C) server and makes itself available to perform additional functions.

This allows a remote attacker to command the Trojan to download and execute further files, shutdown or reboot the computer, or even delete system files, rendering the computer unusable without reinstalling the operating system.

Part 4: Prevention

1. User behavior and precautions

The spam email campaigns used by attackers attempt to trick the user by referencing the latest news stories, playing upon fears that their sensitive information has been stolen, suggesting that compromising photos have been taken of them, or any number of other ruses. Users should use caution when clicking links in such emails.

Basic checks such as hovering with the mouse pointer over each link will normally show where the link leads. Users can also check online Web site rating services such as safeweb.norton.com to see if the site is deemed safe to visit.

2. Patch operating system and software

The attackers behind this threat have been known to utilize exploit packs in order to craft Web pages to exploit vulnerable computers and to infect them with Trojan.Zbot.