Write-up 1

Kevin

March 9-14, 2014

Papers read this week:

1. Borgaonkar, *An Analysis of the Asprox Botnet*[1]

   The researcher performed a static analysis of the Asprox botnet using the tool Norman SandBox Analyzer Pro. Asprox is a C&C botnet that first appeared in 2003. This article focuses on a variant that was found in 2008.

   Key features:

   - C&C structure

     When communicating with the control centre, the Asprox bots send data in the form of a forum post through HTTP. While doing this it also downloads updates, like a file named `COMMON.BIN` that contains a list of IP addresses for the C&C server along with DNS-related information. It also pulls a javascript file that is injected to webpages in an attempt to expand the botnet. This file redirects any potential visitor to a website that will prompt them to install the Asprox binary.

   - Fast-flux Service

     In order to keep the C&C server safe from any potential attackers, a fast-flux technique is employed. The authoritative or name server records of the domain is changed very often and quickly and in so doing the IP address also changes when the domain name is resolved. Since the bots will download a list of alternate IP addresses to communicate with, taking down one server does not affect its operation.

   - Social Engineering

     One of the ways that the Asprox botnet spreads is by pretending that it is some real software that a user might install, for example a codec. It also attempts to have users install it by showing a fake warning message to them and forcing them to install the Antivirus XP 2008 program. Other methods include showing some news articles that are geographically relevant to the user and tricking them into installing a 'new version of flash player' or similar binary which will add them to the botnet.

- SQL Injection[1]

  Since 2008, machines infected with Asprox downloaded a SQL injection attack utility to aid in its spread. This tool searches Google for SQL servers that server .ASP pages, and attempts to take control of it through SQL injection attacks. On a successful attack, the program will inject the aforementioned javascript file into various pages served by the server.

- Lack of Cryptography

  Asprox does not use any form of cryptography in its communications. It also (see above) sends its data in plaintext through HTTP.

An empirical study of a live botnet is useful since it gives us an idea of how real-world botnets might defend themselves. The paper gives insight into how this botnet propagates itself and what methods it employs in order to prevent its compromise.

References

[1] R. Borgaonkar. "An Analysis of the Asprox Botnet". In: *Emerging Security Information Systems and Technologies (SECURWARE), 2010 Fourth International Conference on*. July 2010, pp. 148–153. DOI: 10.1109/SECURWARE.2010.32.

[1] This part seemed the most interesting to me