Spamcraft

An Inside Look At Spam Campaign Orchestration

Presented at: the 2nd Usenix Workshop on Large-Scale Exploits and Emergent Threats (2009)

Paper Authored by:
Christian Kreibich, Chris Kanich, Kirill Levchenko, Brandon Enright,
Geoffrey M. Voelker, Vern Paxson, Stefan Savage

A presentation by: Bryce Van Dyk

[Online] Available: http://www.usenix.org/events/leet09/tech/full_papers/kreibich/kreibich.pdf [Accessed: Sept. 19, 2009]

Overview

- The Storm: once a prominent spamming platform
- Tiered structure:
  - *Worker bots->Proxy bots->HTTP proxies->Bot-master*
- A “command & control” (C&C) protocol is used for communication within botnets. In this paper C&C refers to communication between worker and proxy bots of the Storm.
  - The authors intercepted and modified C&C messages for the purposes of collecting data.

A critique

"Our measurements are driven by a combination of probing and infiltration of the Storm botnet. This network appeared in 2006 and by 2007 had grown to be one of the dominant spamming platforms. By mid-2008 its size had dwindled, and on 21 September 2008 it fell silent when its hosted infrastructure was taken off-line." – First paragraph of section 3

A lack of citation makes this introduction to the Storm difficult to verify. The first sentence implies the authors have some knowledge to base their claims on, but a deficit of other evidence leaves the reader unable to check the validity of the statements made.

Continued critque

- Why had the Storm's size dwindled?
  - Attacks? Competing botnets? Bot-master moving on? Parts being sold? Computers being secured?
- Why was the hosted infrastructure taken offline?
  - Was it attacked? By whom?
    - Academics? Security professionals? Bot-masters?
    - Were the authors of this paper involved?
  - Did the bot-master move on to another botnet?
  - Was it linked to the dwindling size?

Continued Critque

- Do the authors have an interest in intentionally being vague about details?
  - If someone else, especially other researchers, ‘killed’ the Storm, it may overshadow this research. It also raises the questions about why the authors weren’t involved.
  - If the Storm is dead then the application of this research is somewhat diminished.
    - Do people want to read as much about the behaviour of a botnet that no longer functions?

But Some Praise Also

- The researchers actively tampering with the communications of the botnet.
  - Injection of marker emails allows for tracking of information within the Storm. This gives an insight into the botnet's handling of harvested emails.
  - Researchers show that the botnet's traffic can be corrupted. This is useful for future attacks and manipulations (though less so if the Storm is dead).
  - Cloak and dagger: a sense of the tables being turned on the attacker. A degree of poetic justice adds interest to the paper.

Question

- The authors of this paper have been interfering with the Storm by modifying its traffic. Other powers act in more disruptive ways (e.g. Registries preemptively shutting down domains used by Conficker).

- Do these groups have a long term motivation to continue doing so?