What Are Botnets and How to Hijack Them?

Vahab Pournaghshband
Computer Science Department
University of California, Los Angeles
vahab@cs.ucla.edu

Botnets are networks of malware-infected machines controlled by an adversary called botmaster. Each infected machine is called a bot. While there have been many infamous bots that attempted to infect as many machines as possible, there are some bots that infect only specific machines with the aim of stealing valuable information while staying undetected. University of California, at Santa Barbara (UCSB) researchers managed to hijack botnet Torpig for ten days and further analyze the botnet activities, before they lose control when the botnet got updated by the botmaster.

Torpig's victims are infected through drive-by-download attacks, meaning that they need to download and run a trojan (which can be done via various ways). Once the machine is infected, it acts as an installer for the Mebroot which is a toolkit used to replace Master Boot Record (MBR). This has two advantages: (1) it starts the malware at the boot time, and (2) it could potentially remain undetected by antiviruses. The victim's machine then gets rebooted after a few minutes and the program is then loaded. Mebroot, at this initial stage, does not contain any malicious code; however, it facilitates installing, reinstalling, and updating modules. It contacts the Command and Control (C&C) servers to get the modules and then stores them encrypted (under the `system32` directory) in the infected machine. Every 20 minutes the C&C server asks the bot in the victim's machine to upload the stolen data, and then the bot sends the encrypted version of this data to the server. Note that the cryptosystem used by Torpig has been broken in late 2008 and thus UCSD researchers decryption was rather automated. It also often uses phishing to gather more valuable information from the victim. They also use techniques like domain flux to remain undetected while communicating

with the C&C server. All bots communicate with the Torpig's C&C server through `HTTP POST` requests. The URL containing the request includes the bot's ID and a submission header. The payload is just the encrypted stolen data from the victim.

What UCSB researcher did to successfully take control over the bot was by purchasing the domains that the bots try to resolve as a tool to communicate with C&C servers. The researchers then setup C&C servers to communicate with the bots. Although they had control over the bot and could potentially extract any information they needed to further analyze the bot, they were limited to which commands they could issue due to privacy and legal issues involved with the results of those operations.

Now that we know how Torpig botnet infects the machines, it is worth mentioning the potential threats that it can impose on the victims. From data reported by the infected machines, it is clear that the primary motivation behind Torpig is financial data stealing. The statistics the UCSB researchers gathered shows that so many credit card information have been stolen by the bots and were reported to the botmaster. *Man-in-the-browser* phishing attack was one of the most effective techniques that Torpig used to gather valuable information from the victim. It is done in a way that the user under attack observes a valid domain and even SSL certificate looks valid. Password analysis is considered another form of threat to the victims. A remarkable analysis by UCSB researchers shows that Torpig stole around 300,000 unique credentials (i.e. username and password pairs) most from Google, facebook, Yahoo, MySpace, and other social networking and e-mail websites. Privacy is also a form of threat from Torpig since a trace of online activities of the users of infected machines could be available to the botmaster. Other information about the users like their habits, interests, and concerns could be potentially extracted and reported to the botmaster. Once accessing to the stolen data in that ten days, the researchers were able to even classify the victims by their primary activities on the web. The last and not least threat is the denial of service attack by Torpig due the overwhelming usage of aggregate bandwidth among infected hosts.

References

[1] Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., Kruegel, C., and Vigna, G. *Your botnet is my botnet: analysis of a botnet takeover*. In Proceedings of the 16th ACM Conference on Computer and Communications Security (Chicago, Illinois, USA, November 09 - 13, 2009). CCS '09. ACM, New York, NY, 635-647.