Your Botnet is My Botnet: Analysis of a Botnet Takeover

Summary: In this paper, a comprehensive analysis of the operations of the Torpig botnet is discussed. Researchers took control of the Torpig botnet and studied its operations for a period of ten days. During this time, more than 180 thousand infections were detected and almost 70 GB of data was recorded that the bots collected. Botnets are becoming a large problem for the internet. They are formed by networks of compromised computers or bots that are under the control of a "bot master". Botnets are becoming the primary means for criminals to launch DDOS attacks, send spam emails, steal financial and personal data, or other cyber crimes. Torpig is a malware program that is designed to harvest sensitive information (such as bank account and credit card data) from its victims. It has been distributed to its victim as a part of Mebroot. Victims are infected through vulnerable websites which are modified with html tags that causes victims browser to run JavaScript code. If JavaScript's execution is successfully, it downloads an exe file without users knowledge (drive-by-download). This exe acts as an installer for Mebroot. Mebroot does not perform any malicious attacks itself, it acts as a platform to install malicious modules. Once installed, Mebroot contacts the Mebroot C&C server to obtain malicious modules. These modules are saved in encrypted form in the system32 directory, so that, if the user reboots the machine, they can be immediately reused without having to contact the C&C server again. Mebroot contacts its C&C server periodically, to report its current configuration and to potentially receive updates. All communication with the C&C server occurs via HTTP requests and responses and is encrypted using a sophisticated, custom encryption algorithm. Correspondence with C&C server is achieved through domain flux - using a domain generation algorithm (DGA) to locate active C&C servers. Mebroot injects these modules into a number of applications so that it can inspect / steal all the data handled by these programs. Torpig was hacked by reverse engineering the DGA which resulted in a three week span of unregistered domains. These domains were registered and acted as the C&C center. By providing a valid response, the bots accepted the server as genuine, and the entire system was hacked. Analysis of data showed that bots communicated with the Torpig C&C through HTTP POST requests. The URL used for this request contains the hexadecimal representation of the bot id and a submission header. The body of the request contains the data stolen from the victim's machine. To measure size of the botnet, bot id was preferred over IP address due to the NAT and DHCP churn issues.

Opinion: In my opinion this was a major breakthrough against the criminals. In just TEN days, Torpig obtained credentials of 8,310 accounts at 410 different institutions costing around anywhere between $83K and $8.3M. Reverse engineering an algorithm is not an easy task but the researchers were successful in breaking the DGA. This was the crux which helped in hacking the Torpig. Within the past few years, malwares have transformed from a for fun (or notoriety) activity to a for-profit enterprise. Torpig not only steals data but has the potential to drag its victims into a variety of malicious activities.

Advantages: There are a couple of lessons learnt from the analysis. First, victims of botnets are often users with poorly maintained machines that choose easily guessable passwords to protect access to sensitive sites. 38% of the credentials stolen by Torpig were obtained from the password manager of browsers. Secondly, reuse of credentials should be avoided. Analysis of passwords showed that 28% of the victims reused the credentials. This helps botnets to shoot two birds with the same stone.