B4 StealthBots: A Digital Forensics Case Study

Cory Nguyen, MSc, and Marcus Rogers, PhD, Purdue Univ, Dept of Computer and IT, 401 N Grant St, West Lafayette, IN 47907*

After attending the presentation, the attendees will be able to understand the impact that stealthbots have on digital investigations, detect footprints of a stealthbot in the file system, and explain the defense strategy that is being proffered regarding stealthbots.

This presentation will impact the forensic science community by highlighting the challenges of investigations where the stealthbot defense, almost impossible to disprove at this time, is used.

As the legal justice system becomes better educated and mature in the domain of digital investigations, standard defense strategies are appearing. One such strategy is to blame someone else. A more sophisticated expansion on this legal defense is that while the system belonging to the accused was used to perpetrate the crime, the accused was not the one sitting behind the keyboard, or was "framed" by some unknown entity. To date this defense has met with minimal success. With the introduction of stealth malware such as the Zeus bot Stealth (Zbot-Stealth) into the "wild," this defense takes on a entirely new dimension.

The Zbots have been primarily used by the criminal community to attack online banking systems. These bots have become increasingly sophisticated and can be modified to attack particular banks. The bots are "made to hire" and can be purchased online from the developers for prices ranging from $2,000 to $20,000 USD. The complex nature of these "made to order" malware programs has made the detection and investigation of cases more difficult. However, these bots tended to leave "footprints" in file systems that could be discovered and readily identified as malware. The anti-virus industry has also developed detection and removal capabilities related specifically to bots.

Recently, a new variant of the Zbot was released that has been coded to implement stealth and anti-forensics. The anti-forensics capabilities, while not technically new, allow the program to remove its traces from the infected system and obfuscate any remnants showing it was ever installed. The Zbot-stealth variants appear to be very effective at erasing all traces in the file system that they were ever installed and/or executed on the infected system. The real novelty of the stealth variant is its ability to take control of the victim's system at the same time that the victim is still logged in and using the system. This is very unique. Prior variants relied on the standard Remote Desktop Protocol (RDP) and Virtual Network Computing (VNC) to gain access and control of the victim's system. Using the standard method of RDP, the system would terminate the access of any user logged on locally and hand over control to the remote user. This meant that the victim would be able to detect that a remote control session had occurred. The new variants have modified or "hacked" the RDP protocol and now control of the system can be gained remotely without the local logged-in user being logged-out. Now the attacker can easily "piggyback" on the victim's activity and orchestrate an attack from the victim's system with the victim still using the system. The resulting traces of the attack and the victim's normal system usage behavior become co-mingled and extremely difficult to differentiate.

The presentation will discuss the technical aspects of the Zbot-Stealth variant, the forensic challenges associated with the new attack vector used by the malware, and how to effectively examine and analyze a system that may have been infected. A case study will briefly be introduced where the Zbot-stealth defense was put forward. The case study highlights the difficulty in countering this defense given the lack of positive forensic evidence left in the digital crime scene by this new class of attacks.

Bots, Stealth, Digital

 ** Presenting Author*