C30 A New Botnet Command and Control Mechanism Using the Ethereum Platform

Joshua Ralls, Eastern Kentucky University, Richmond, KY 40475; Shuangteng Zhang, PhD, Eastern Kentucky University, Richmond, KY 40475*

Learning Overview: After attending this presentation, attendees will have a better understanding of botnets, Command and Control (C&C) servers, and blockchain technology, as well as the possible use of the Ethereum platform to create botnet C&C server to automatically launch cyberattacks, such as ransomware attacks, and the corresponding possible countermeasures against these attacks.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by introducing a possible new cyber attacking approach that takes advantage of the blockchain technology, which can make the attacks more difficult to track and shut down, and through discussing the corresponding defending and investigation strategies on these types of attacks.

Botnets are a group of compromised internet-connected machines remotely controlled by the botmaster that serves as the C&C server to send commands to and receive information from the bots, the individual machines consisting of the botnet. Using botmaster and botnets, the malicious users can launch Distributed Denial-of-Service (DDoS) attacks, spread malware such as ransomware, distribute spam, steal data, and more. To successfully take down or disrupt the operations of the botmaster and botnet, bots are usually analyzed to trace and discover the botmaster and the bot network.

The current botnet attacking relies on the botmaster with a centralized management. Therefore, the botmaster becomes the weakest point of botnet infrastructure. Once the botmaster is discovered, many takedown techniques can be used to counteract the operations between botmaster and the bots. To avoid the botmaster from being revealed, many techniques such as HTTP botnets, domain flux, and peer-to-peer botnets are used by malicious users. However, even with these techniques, the botmaster and botnets are still traceable and can be taken down or disrupted.

Blockchain technology provides a new way of storing information in a distributed ledger that allows a reliable and secure sharing of and access to the same information. This technology can be applied to numerous applications for good purposes. However, because of its decentralized management of information, blockchain technology may possibly be used by the malicious users to build a botmaster and botnet infrastructure and make it, if not impossible, at least difficult to trace and take down.

Botnets, Command & Control Server, Ethereum