Stegoloader Malware hides exploit code in images Dell SecureWorks Counter Threat Unit™ Threat Intelligence unit has released information about Stegoloader. Appearing to have been active since 2012, this particular malware uses digital steganography – the art of hiding secret information within a digital image or graphic – to conceal its true nature and to avoid detection.

Stegoloader operators are hiding a core component of the malware within a portable network graphic (PNG) hosted on a legitimate site. As Stegoloader executes, it downloads the core component and then uses digital steganography to extract the code from the image. The core component is never saved to the victim's computer, meaning that it is incredibly difficult to detect the malware through regular tools.

Szilard Stange, director, OPSWAT notes;

"Malware authors are always looking for new distribution mechanism to make detection harder, however modern internet security desktop suites contain methods to detect unusual network operations even when the remote site is a well known site. They are also able to track what the running processes exactly does. It means that detection of malware like Stegoloader can be harder but not impossible. There are many ways to deliver harmful content including this steganography based one but there are other interesting way to distribute harmful code like embedded data into DNS queries/responses. Any of them can be in main-stream but it mainly depends how anti-malware vendors can react to these attacks. To protect an organization against attacks like this one it is worth to consider applying data sanitization techniques to remove any harmful content from images downloaded from the internet without losing important data."

Martin Lee, intelligence manager, Alert Logic states;

"We are currently in an arms race between malware writers and the security industry. As security researchers become more adept in discovering malware, so malware writers must become more inventive in hiding their malware. In many ways, seeing malware writers deploying inventive strategies to disguise and hide their malware is proof that security solutions are making it difficult for malware to persist and that we are forcing malware writers to innovate. Even if this malware is hiding itself on the end point, the command and control traffic is still visible on the network. Monitoring for traffic to known command and control servers or anomalous traffic remains an excellent technique for identifying the presence of malware, even if identifying and reverse engineering the malware becomes more difficult."