Detecting Malicious Http Users Using The Community Structure Property In Interaction Graph

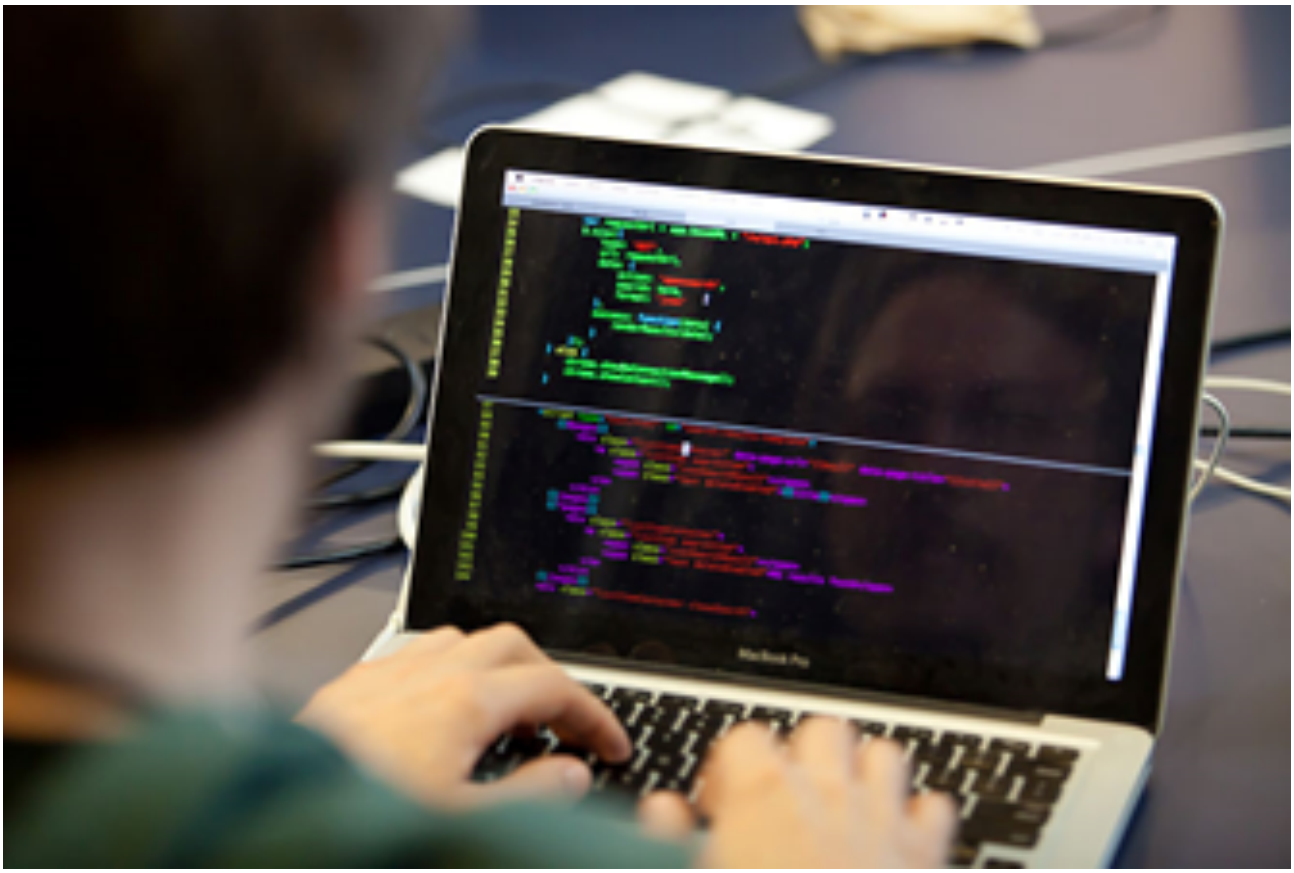
Published date: March 23, 2017

Technology description

Background:
Wealth is being transferred into the hands of malicious cybercriminals with an estimated annual global cost of $445B from Intellectual Property (IP) theft. The security industry needs to rapidly progress to keep up with the ever more innovating cybercrimes. Due to the inadequacy of traditional security scanning software, we need a better method that is proficient in detecting perpetrators before they gain access to confidential information.
Brief Description:
Malicious HTTP scanners scan for vulnerable websites with easy access into private information. UCR researchers created Scanner Hunter, a reconnaissance tool that will enable them to take preemptive measures before actual infiltration occurs. The tool has an innovative approach of filtering HTTP requests and tagging them as malignant or benign. Their dynamic methodology and algorithm successfully achieves its functions with 96.5% accuracy while virtually eliminating all false-positives.

Additional Information

Images



Wikimedia Commons /http://commons.wikimedia.org/wiki/File:ImagesCABNLU5S.jpg
Wikimedia Commons /http://commons.wikimedia.org/wiki/File:Typing_computer_screen_reflection.jpg

Application area

Government agencies – fraud, identity theft
Security system companies
Internet service providers
IT companies
Tracking software companies

Advantages

Detects HTTP scanners with 96.5% precision– better than existing methodologies
Differentiates between legitimate HTTP requests and stealthy requests

Institution

University of California, Riverside

Inventors

Guowu Xie
Michalis Faloutsos
Huy Hang