New tool skewers socially engineered attack ads

September 11 2023, by John Popham

Credit: Pixabay/CC0 Public Domain

"Warning! Your computer is infected with a virus. Click the button below to take immediate action!"

Online ads like this are all too familiar and often the opening salvo in personal cyberattacks that can lead to unwanted software or other malicious downloads.

Georgia Tech researchers are countering deceptive online ads with a pioneering solution designed to challenge the rising threat of online social engineering attacks by cutting them off at the source.

Trident, created by Ph.D. student Zheng Yang and his team of researchers, is an add-on compatible with Google Chrome that has proven to block these ads with nearly 100% efficiency.

Advertisements are fertile ground for scams and fraudulent schemes. While such networks may offer better pay to websites than industry giants like Google and Facebook, their advertisements often employ tactics that lure unsuspecting users into compromising situations.

"The goal is to identify suspicious ads that often take users to malicious websites or trigger unwanted software downloads," said Yang. "Trident operates within Chrome's developer tools and uses a sophisticated AI to assess potential threats."

The team compiled a vast dataset from more than 100,000 websites to build Trident, including 10 low-tier ad networks. This comprehensive data collection helped identify 1,479 instances of attacks encompassing a range of six common types of web-based social engineering attacks. These include:

- Tech-support scams
- Unwanted software downloads
- Scareware
- Dating scams
- Notification spam
- Prize scams

The remarkable outcome of their efforts is the sustained performance of Trident. Over the course of a year, the tool consistently achieved a nearly

perfect detection rate of malicious ads, ensuring users' safety by minimizing the risk of interacting with harmful content.

Impressively, this achievement came with a meager 2.57% false positive rate, demonstrating the accuracy and effectiveness of Trident's machine-learning capabilities.

TRIDENT: Towards Detecting and Mitigating Web-based Social Engineering Attacks was presented at the 32nd USENIX Security Symposium in August. Contributors to this project include Georgia Tech Ph.D. students Joey Allen and Matthew Landen, Adjunct Assistant Professor Roberto Perdisci, and Professor Wenke Lee.

More information: TRIDENT: Towards Detecting and Mitigating Web-based Social Engineering Attacks.
www.usenix.org/conference/usen … sentation/yang-zheng

Provided by Georgia Institute of Technology

Citation: New tool skewers socially engineered attack ads (2023, September 11) retrieved 8 December 2023 from https://techxplore.com/news/2023-09-tool-skewers-socially-ads.html