16 Mar 2017

CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data (1:10-1:50 pm ET)

and

Transfer Learning for Network Security (2:00-2:40 pm ET)

Mark your calendars and come join your friends in the CAE community for a Tech Talk. We are a warm group that shares technical knowledge. CAE Tech Talks are free and conducted live in real-time over the Internet so no travel is required. You can attend from just about anywhere (office, home, etc.) Capitol Technology University (CTU) hosts the presentations using their online delivery platform (Adobe Connect) which employs slides, VOIP, and chat for live interaction. Just log in as "Guest" and enjoy the presentation(s).

Below is a description of the presentation(s) and logistics of attendance:

Date: Thursday 16 Mar 2017

Time: 1:10-1:50 pm ET

Location: https://capitol.adobeconnect.com/cae_tech_talk/

Just log in as "Guest" and enter your name. No password required.

Title/Topic: CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data

Audience Skill Level: All Levels

Presenter(s): Nolen Scaife (University of Florida)

Description:

Ransomware is a growing threat that encrypts a user's files and holds the decryption key until a ransom is paid by the victim. This type of malware is responsible for tens of millions of dollars in extortion annually. Worse still, developing new variants is trivial, facilitating the evasion of many antivirus and intrusion detection systems. This talk presents CryptoDrop, an early-warning detection system that alerts a user during suspicious file activity. Using a set of behavior indicators, CryptoDrop can halt a process that appears to be tampering with a large amount of the user's data. Furthermore, by combining a set of indicators common to ransomware, the system can be parameterized for rapid detection with low false positives. Our experimental analysis of CryptoDrop shows it stops ransomware from executing with a median loss of only 10 files (out of nearly 5,100 available files). Our results show that careful analysis of ransomware behavior can produce an effective detection system that significantly mitigates the amount of victim data loss.

Date: Thursday 16 Mar 2017

Time: 2:00-2:40 pm ET

Location: https://capitol.adobeconnect.com/cae_tech_talk/

Just log in as "Guest" and enter your name. No password required.

Title/Topic: Transfer Learning for Network Security

Audience Skill Level: Intermediate

Presenter: Dr. Sachin Shetty (Old Dominion University)

Description:

Machine learning techniques have been employed in detecting occurrence of malicious attack and classification of malware families. Most machine techniques for malware detection are effective in building classifiers in the presence of labeled dataset. The availability of labeled dataset also hinges on the assumption that we can build predictive models of dynamic threats based on prior models of adversarial behavior. At the same time it is time consuming and impractical to generate labeled dataset.
In this talk, I will techniques that builds on existing models of adversarial behavior to extend to environments characterized by diversity of systems, networks and users. Specifically, I will discuss transfer learning technique to detect threats to computer systems and networks. Transfer learning utilizes labeled data in a source domain to help to train better models in the target domain with insufficient or no labels. To the best of our knowledge, this is the first effort to use a feature-based transfer learning technique to detect malware. The premise of the technique is to find a common latent feature subspace for the source and target domain by

minimizing the difference between the data distributions while preserving the original discriminative data far apart. The technique can project the source and target data onto the new latent subspace. Furthermore, this technique can be used with any type of classifier on the transformed source data and does not need labeled target data. We evaluated the technique on publicly available datasets and results demonstrate the effectiveness of transfer learning to detect network attacks.

CAE Tech Talks are also recorded

Recordings of live presentations are posted to the website below:

https://capitol.instructure.com/courses/510/external_tools/66

Pdf versions of the presentations are posted to the website below:

https://capitol.instructure.com/courses/510/files

Contact

CAE Tech Talk events are advertised thru email and posted to the news and calendar section of the CAE community website: www.caecommunity.org

For questions on CAE Tech Talk, please send email to CAETechTalk@nsa.gov