Scientists stop and search malware hidden in shortened urls on Twitter

September 25 2015

Cyber-criminals are taking advantage of real-world events with high volumes of traffic on Twitter in order to post links to websites which contain malware.

To combat the threat, computer scientists have created an intelligent system to identify malicious links disguised in shortened urls on Twitter. They will test the system in the European Football Championships next summer. The research is co-funded by the Engineering and Physical Sciences Research Council (EPSRC) and the Economic and Social

Research Council (ESRC).

In the recent study the Cardiff University team identified potential cyber-attacks within five seconds with up to 83% accuracy and within 30 seconds with up to 98% accuracy, when a user clicked on a URL posted on Twitter and malware began to infect the device.

The scientists collected tweets containing URLs during the 2015 Superbowl and cricket world cup finals, and monitored interactions between a website and a user's device to recognise the features of a malicious attack. Where changes were made to a user's machine such as new processes created, registry files modified or files tampered with, these showed a malicious attack.

The team subsequently used system activity such as bytes and packets exchanged between device and remote endpoint, processor use and network adapter status to train a machine classifier to recognise predictive signals that can distinguish between malicious and benign URLs.

Dr Pete Burnap, Director of the Social Data Science Lab at Cardiff University, and lead scientist on the research, said: "Unfortunately the high volume of traffic around large scale events creates a perfect environment for Cyber-criminals to launch surreptitious attacks. It is well known that people use online social networks such as Twitter to find information about an event.

"Attackers can hide links to malicious servers in a post masquerading as an attractive or informative piece of information about the event.

"URLs are always shortened on Twitter due to character limitations in posts, so it's incredibly difficult to know which are legitimate. Once infected the malware can turn your computer into a zombie computer

and become part of a global network of machines used to hide information or route further attacks.

"In a 2013 report from Microsoft these 'drive-by downloads' were identified as one of the most active and commercial risks to Cyber security.

"At the moment many existing anti-virus solutions identify malware using known code signatures, which make it difficult to detect previous unseen attacks."

Professor Omer Rana, Principal investigator on the project which is also includes Royal Holloway, University of London, City University London, the University of Plymouth and Durham University said:

"We are trying to build systems that can help law enforcement authorities make decisions in a changing Cyber Security landscape. Social media adds a whole new dimension to network security risk. This work contributes to new insight into this and we hope to take this forward and develop a real-time system that can protect users as they search for information about real-world events using new forms of information sources.

"We have the European Football Championships coming up next summer, which will provide a huge spike in Twitter traffic and we expect to stress-test our system using this event."

Professor Philip Nelson, Chief Executive, EPSRC said: "Using social media is an integral part of modern life, vital to organisations, businesses and individuals. The UK needs to operate in a resilient and secure environment and this research will help combat these criminal Cyber-attacks."

More information: "Real-time Classicfication of Malicious URLs n Twitter using Machine Activity Data" presented at 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining in August 2015. The study authors are Pete Burnap, Amir Javed, Omer F. Rana, Malik S. Awan. School of Computer Science and Informatics, Cardiff University

Provided by Engineering and Physical Sciences Research Council (EPSRC)