Hidden cyber threats revealed with new visualization software Eventpad

The destruction of a nuclear facility in Iran; 6.5 million user credentials stolen from LinkedIn; the nationwide attack on the German parliament. These are just a few examples of headlines that occur almost daily on international television and newspapers. Cyber-attacks are getting more complex targeting specific infrastructures while trying to hide their malicious activity in computer networks. Researcher Bram Cappers took on this challenge and designed new type of cybersecurity software that discovers hidden patterns in computer viruses by synergizing visualization and artificial intelligence in one system.

In contrast to traditional viruses, targeted cyber threats are designed to strike once and can take months of preparation in order to succeed. We cannot wait until the attack has happened in order to identify them. Only by actively monitoring our systems and computer networks are we able to detect signs of undesired activity. This involves the analysis of patterns and outliers in data sources such as network traffic, user behavior, activity logs etc.

During his PhD Cappers developed a new type of data analysis software called Eventpad to visually detect (malicious) patterns and outliers inside computer networks and event logs. It does this by visualizing system events such as network traffic, electronic health records, or file access as blocks on a screen. Combined with automated techniques, find&replace functionality, and color rules users can quickly search and highlight outliers in the data.

Current intrusion detection software use complex algorithms to automatically discover threats in these system events. However, in practice these algorithms still generate a lot of false alerts due to the lack of background knowledge. After all, events can only tell what has happened and not why. Human-analysis is still required afterwards to separate false alerts from the critical ones. The complexity of these algorithms however often makes it difficult to understand why they have been generated in the first place.

With Eventpad we solve this problem by working the other way around. We start with the user highlighting properties that he is interested in. Automatic techniques in turn can use this information to steer the user to other (unknown) patterns of interest. Interestingly, this technique does not limit itself to security, but can also be applied to other domains such as Healthcare and fraud detection.

The research of Cappers has made a lot of traction in both industry and academia. Besides winning the IEEE Visual Analytics Challenge in 2017 with record speed and the ICT.Open award for Best Demo, Eventpad has been successfully applied for the detection of fraud in Voice Over IP telephony, the discovery of bottlenecks in a radiology department and the reverse engineering of ransomware viruses at the university. In addition, the technology has been presented at prestigious industrial events including Black Hat USA 2018, Still Hacking Anyway 2017 and has been published in the European Cyber Security Perspectives as new and innovative technology in cybersecurity.

The research is an important step towards building more secure systems by understanding how they should behave rather than to fully rely on artificial intelligence. Human knowledge still plays a crucial role in the discovery of cyber threats. In the end it is always possible to find outliers and threats in your system. The main challenge is to find the ones that matter the most for your security.