CyLab researchers create network traffic visualization tool to help thwart cyber attacks

November 7 2016

Last month, tens of websites including Amazon, Netflix and others fell victim to one of the largest distributed denial of service (DDoS) attacks in history, temporarily crashing under the weight of huge amounts of fake traffic orchestrated by malicious hackers. At Carnegie Mellon, research out of the CyLab Security and Privacy Institute shows that the tools needed to thwart these kinds of attacks are on the horizon.

"Lots of network traffic data is collected in the form of static reports, but it is very overwhelming for an analyst to digest those data," says Yang Cai, a senior systems scientist who directs CyLab's Visual Intelligence Studio. "Visualization is one way to change abstract data into pictures, sound, and videos so you can see patterns in a very intuitive way."

Cai and his colleague Sebastian Peryt have created a tool that allows one to visualize network traffic to more easily identify key changes and patterns. The researchers have used this tool to inspect network traffic during DDoS attacks and map out the structure of malware distribution networks.

Last week, the researchers presented the tool's application in visualizing malware distribution networks at the IEEE Symposium on Visualization for Cybersecurity in Baltimore, MD. A video demonstrating the tool can be viewed here.

"Based on these visualization graphs, analysts can focus on critical areas

to help shut down a malware distribution network, or in the case of a DDoS attack, target a critical node to thwart the attack," says Peryt, a research assistant in CyLab.

Moving forward, the team aims to consider human factors in making the tool more usable, operate more efficiently, and to integrate it into a virtual reality platform so analysts can more easily explore the graphs with intuitive motions.

Provided by Carnegie Mellon University