Catching hackers in the act

October 7, 2018

Catching hackers in the act

by Juston Moore

In May, the FBI issued a warning to owners of home routers that their devices might have fallen prey to a malware attack by a group of hackers with ties to the Russian military.

The malware, called VPNFilter, allowed hackers to collect personal information and attack other devices. This attack was notable for its breadth — but it certainly wasn’t unique. An estimated 5.99 billion malware attacks took place in the first half of 2018 alone.

At Los Alamos National Laboratory, where some of the nation’s most precious secrets are kept, information is not only closely guarded, tools are being developed to help others detect and respond quickly to targeted attacks.

Understanding the capabilities and intent of malware — a process known as reverse engineering — is a difficult, manual process that can take days or even weeks for an expert analyst. Los Alamos has long been a leader in manual malware analysis, and has found that expert intuition can be augmented by machine learning tools that rapidly identify patterns across large sets of related malware, collected over time.

This story first appeared in Santa Fe New Mexican.

Managed by Triad National Security, LLC for the U.S Department of Energy's NNSA