Los Alamos
NATIONAL LABORATORY
EST 1943

Foiling illicit cryptocurrency mining with artificial intelligence

August 20, 2020

LOS ALAMOS, N.M., Aug. 20, 2020—Los Alamos National Laboratory computer scientists have developed a new artificial intelligence (AI) system that may be able to identify malicious codes that hijack supercomputers to mine for cryptocurrency such as Bitcoin and Monero.

“Based on recent computer break-ins in Europe and elsewhere, this type of software watchdog will soon be crucial to prevent cryptocurrency miners from hacking into high-performance computing facilities and stealing precious computing resources,” said Gopinath Chennupati, a researcher at Los Alamos National Laboratory and co-author of a new paper in the journal *IEEE Access*. “Our deep learning artificial intelligence model is designed to detect the abusive use of supercomputers specifically for the purpose of cryptocurrency mining.”

Cryptocurrencies, such as Bitcoin, are forms of digital money. Instead of minting it like coins or paper bills, cryptocurrency miners digitally dig for the currency by performing computationally intense calculations.

Legitimate cryptocurrency miners often assemble enormous computer arrays dedicated to digging up the digital cash. Less savory miners have found they can strike it rich by hijacking supercomputers, provided they can keep their efforts hidden. The new AI system is designed to catch them in the act by comparing programs based on graphs, which are like fingerprints for software.

All programs can be represented by graphs that consist of nodes linked by lines, loops, or jumps. Much as human criminals can be caught by comparing the whorls and arcs on their fingertips to records in a fingerprint database, the new AI system compares the contours in a program’s flow-control graph to a catalog of graphs for programs that are allowed to run on a given computer.

Instead of finding a match to a known criminal program, however, the system checks to determine whether a graph is among those that identify programs that are supposed to be running on the system.

The researchers tested their system by comparing a known, benign code to an abusive, Bitcoin mining code. They found that their system identified the illicit mining operation much quicker and more reliably than conventional, non-AI analyses.

Because the approach relies on graph comparisons, it cannot be fooled by common techniques that illicit cryptocurrency miners use to disguise their codes, such as including obfuscating variables and comments intended to make the codes look like legitimate programming.

While this graph-based approach may not offer a completely foolproof solution for all scenarios, it significantly expands the set of effective approaches for cyber detectives to use in their ongoing efforts to stifle cyber criminals.

Based on recent computer break-ins, such software watchdogs will soon be crucial to prevent cryptocurrency miners from hacking into high-performance computing facilities and stealing precious computing resources

The research appeared July 27, 2020 in the journal *IEEE Access.*

Publication: Code Characterization with Graph Convolutions and Capsule Networks, Poornima Haridas, Gopinath Chennupati, Nandakishore Santhi, Phillip Romero, Stephan Eidenbenz, IEEE Access, DOI: 10.1109/ACCESS.2020.3011909