Simulated computer network alters reality to mislead hackers

November 29 2017

Sandia National Laboratories cyber researcher Vince Urias helped develop the Sandia-originated HADES program that employs alternative realities to confuse hackers. HADES stands for High-fidelity Adaptive Deception & Emulation System. Credit: Randy Montoya

The Russian novelist Fyodor Dostoevsky once postulated that the devil

no longer uses fire and brimstone but instead simply tells you what you want to hear.

Sandia National Laboratories cyber researchers go with that second option when it comes to foiling a hacker. Rather than simply blocking a discovered intruder, Vince Urias, Will Stout and Caleb Loverro deploy a recently patented alternative reality, dubbed HADES for High-fidelity Adaptive Deception & Emulation System, which feeds a hacker not what he needs to know but what he wants to believe.

"Deception is the future of cyber defense," said Urias. "Simply kicking a hacker out is next to useless. The hacker has asymmetry on his side; we have to guard a hundred possible entry points and a hacker only needs to penetrate one to get in."

Rather than being summarily removed from a data source, a discovered hacker is led unobtrusively into HADES, where cloned virtual hard drives, memory and data sets create a simulation very much like the reality. However, certain artifacts have been deliberately, but not obviously, altered.

"So, a hacker may report to his handler that he or she has cracked our system and will be sending back reports on what we're doing," Urias said. "Let's say they spent 12 months gathering info. When they realize we've altered their reality, they have to wonder at what point did their target start using deception, at what point should they not trust the data? They may have received a year or so of false information before realizing something is wrong. A hacker informing his boss that he's discovered a problem doesn't do his reputation much good, he's discredited. And then the adversary must check all data obtained from us because they don't know when we started falsifying."

Furthermore, when a hacker finally puzzles out something is wrong, he

must display his toolkit as he tries to discern truth from fiction.

"Then he's like a goldfish fluttering in a bowl," said Urias. "He exposes his techniques and we see everything he does."

HADES just won a 2017 R&D100 award, presented by R&D Magazine to recognize exceptional innovations in science and technology over the past year. The Sandia work, patented in October, began five years ago with a three-year Laboratory Directed Research and Development grant.

"It used to be that technologically we couldn't move a visitor to a different reality without them knowing," said Urias, "but there's been a radical change in networking in the last 10 to 15 years, from hardware to software. With the ephemerality of the network fabric, I can change realities without a hacker knowing."

Adversaries want data that helps their situational awareness. "But when we change data in our fake world, we devalue information and set up eventual inconsistencies."

To do this, Urias said, "we move to another location in the cloud and build a slightly different world around them. Our intent is to introduce doubt. If they get something, is it real or is it fake? The worst horror for an adversary is the identical world, but changed. Can we introduce more work for them?"

HADES can operate in multiple modes from a small organization without resources to a large company, he said. The Department of Homeland Security's Cyber Security Division has worked with Sandia on deployment.

Like any technique, HADES has its limitations. While the simplest deceptive environment can be done on a small private computer,

environments of greater fidelity require more CPU and memory resources and may thereby reduce the number of virtual environments deployable on a single server.

What the information technology and cybersecurity communities want, Urias said, is what he wants: "To stop the [information] bleeding, and get actionable intelligence: What is an adversary looking for, what did they actually get, and how did they get it?"

The technique has allowed the researchers to locate malware an adversary has placed in a system, and is capable of active attack.

Provided by Sandia National Laboratories