Malware 'vaccine' generator licensed for cybersecurity platform

March 24 2023

Jared Smith, former ORNL scientist and the inventor of the adversarial malware input generator, or AMIGO, shakes hands with Susan Hubbard, ORNL deputy for science and technology, during an event to celebrate the licensing of AMIGO to Smith's company, Penguin Mustache, on March 21. Credit: Carlos Jones/ORNL, U.S. Dept. of Energy

Access to artificial intelligence and machine learning is rapidly changing technology and product development, leading to more advanced, efficient and personalized applications by leveraging a massive amount

of data.

However, the same abilities also are in the hands of bad actors, who use AI to create malware that evades detection by the algorithms widely employed by network security tools. Government agencies, banking institutions, critical infrastructure, and the world's largest companies and their most used products are increasingly under threat from malware that can evade anti-virus systems, hijack networks, halt operations and expose sensitive and personal information.

A technology developed at the Department of Energy's Oak Ridge National Laboratory and used by the U.S. Naval Information Warfare Systems Command, or NAVWAR, to test the capabilities of commercial security tools has been licensed to cybersecurity firm Penguin Mustache to create its Evasive.ai platform. The company was founded by the technology's creator, former ORNL scientist Jared M. Smith, and his business partner, entrepreneur Brandon Bruce.

"One of ORNL's core missions is to advance the science behind national security," said Susan Hubbard, ORNL's deputy for science and technology. "This technology is the result of our deep AI expertise applied to a big challenge—protecting the nation's cyber- and economic security."

Smith, who worked in ORNL's Cyber Resilience and Intelligence Division for six years, created the technology—the adversarial malware input generator, or AMIGO—at the request of the Department of Defense. AMIGO was created as the evaluation tool for a challenge issued by NAVWAR for AI applications that autonomously detect and quarantine cybersecurity threats. NAVWAR is an operations unit within the Navy that focuses on secure communications and networks.

"ORNL's Cyber Resilience and Intelligence Division is a world leader in

cybersecurity technology," said Moe Khaleel, associate laboratory director for the lab's National Security Sciences Directorate. "Moving AMIGO into the marketplace will help protect our nation's critical infrastructure from attack."

"We put AMIGO to the test in a realistic environment. It's been through the wringer and has been validated at a high technical readiness level," Smith said. "The core technology is designed to build evasive malware, like a virus, that can bypass an existing detection technology."

Mike Paulus, ORNL director of technology transfer, speaks to attendees at an event celebrating the licensing of AMIGO to Penguin Mustache. Credit: Carlos Jones/ORNL, U.S. Dept. of Energy

Drawing on more than 35 million malware samples—some publicly available and others never before seen—AMIGO generates optimally evasive malware in tandem with the training information needed for a security system to detect it in the future.

Smith likens the process to vaccine development. "It's as if we generated a million virus variants and a million vaccines to protect against them—we can collapse that into one vaccine and inoculate everyone. They're protected against the threat, but also all the natural evolutions of the threat going forward."

Luke Koch, who in 2019 worked on the AMIGO development team through the DOE Office of Science's SULI, or Science Undergraduate Laboratory Internship program, is now a doctoral student at the Bredesen Center for Interdisciplinary Research and Graduate Education, a collaboration between ORNL and the University of Tennessee, as well as a graduate research assistant in ORNL's Cybersecurity Research Group. With Smith's direction, Koch wrote the binary instrumentation code used in AMIGO.

"Cybersecurity commercialization is important because our adversaries are always probing for weaknesses throughout the supply chain," Koch said. "One single flaw is all it takes to invalidate a clever and expensive defense."

Amid a growing public understanding of the power of AI, the team is eager to see AMIGO integrated into Evasive.ai and implemented by national security agencies to protect government assets and infrastructure.

"Bad actors are already using artificial intelligence to advance their attacks," Bruce said. "As open AI tools improve, attempts to penetrate security systems will increase in volume and sophistication."

Additionally, long-term use of the Evasive.ai platform could inform a more complete understanding of the mechanisms that contribute to adversarial samples. This insight will make the next generation of machine learning defenses more robust.

And what does any of this have to do with penguins? The company's playful name is a riff on the problem of a small mutation enabling a virus to evade existing defenses—a penguin disguised with a mustache.

Provided by Oak Ridge National Laboratory