STTR SUCCESS STORY

NEW TECHNOLOGY COULD MITIGATE RANSOMWARE ATTACKS

Grant or Contract
STTR Phase I & II

Program Manager
Dr. Cliff Wang

Business
Oceanit Laboratories, Inc.

Type of Business
Small business

Academia
University of Michigan

Commercialization & Tech Transfer
The prototype is being field tested at Michigan Medical and with the U.S. Army's Program Executive Office, Combat Support & Combat Service Support (PEO CS&CSS)

COMPETENCIES
Network, Cyber and Computational Sciences

MODERNIZATION PRIORITIES
Network

A new technology in development could mitigate ransomware attacks and allow for effective recovery when critical data has been breached. Ransomware detection and mitigation is critical for future Army needs in cyber defense.

Ransomware is malicious software that locks a victim's computer files through cryptographic encryption and prevents access until a ransom is paid. The problem continues to escalate each year. According to the EMSISoft, the worldwide costs of ransom demands in 2020 was $75 billion.

"To meet the Army's modernization networking priority, we must ensure the Army's network is safe from malicious software," said Dr. Cliff Wang, program manager, U.S. Army Combat Capabilities Development Command, known as DEVCOM, Army Research Laboratory. "This new technology will allow cyber defenders to deal with malware especially ransomware effectively by identifying these threats and also having a reliable way to recover files locked up by adversaries should it happen."

The project funded by the Army Small Business Technology Transfer program, or STTR, uses external storage devices that are currently not allowed on Army computers because of the threat of malware infection. If successful, this solution would mitigate that issue.

The STTR program is managed by DEVCOM Army Research Laboratory.

Researchers at Oceanit Laboratories, Inc., in collaboration with University of Michigan, are developing intelligent ransomware detection algorithms in USB device firmware to protect a wide range of devices from attacks. The technology employs advanced techniques to stealthily detect malicious actions and automatically create a backup of the original files to a separate and protected location.

"By placing intelligence into the USB device firmware, we can create a universal solution that can protect previous storage devices like CDs and DVDs, current devices like flash memory, and next generation storage technologies to future proof the approach," said David Siu, Cybersecurity Lead at OceanIt Laboratories. "This also allows us to protect other peripherals such as keyboards and mice as well."

The team constructed a laboratory prototype that demonstrates the technology in the form of a USB flash drive. If the drive is connected to a computer that is hit by ransomware, the drive itself detects that it is being encrypted and automatically retains a backup of the original data. All the user needs to do to recover the data is attach the drive to an uninfected computer and press a button and the original, unencrypted data is immediately recovered.

In contrast to the basic research programs managed by DEVCOM ARL, the STTR program focuses primarily on feasibility studies leading to prototype demonstration and productized testing for specific applications. This three-phase program requires a small business to collaborate with a research institution, typically a university or nonprofit research institution.

OceanIt received a Phase I grant in December of 2018 where they initially developed the ransomware detection algorithms without the use of signatures that is commonly employed by anti-virus software.

The technology is currently participating in Phase II. As part of Phase II, the team received up to $1.1 million to spend between six and 18 months developing a demonstration prototype.

As part of Phase II, Michigan Medicine, one of the largest health care complexes in Michigan, will serve as the first customer to field test the technology. They will evaluate the ransomware solution in a real-world environment and provide feedback on operation and performance.

The technology will also be tested with the U.S. Army's Program Executive Office, Combat Support & Combat Service Support via transition partner Lockheed Martin. PEO CS&CSS is a lifecycle management team that provides integrated, tailored, and cost-conscious products to warfighters.

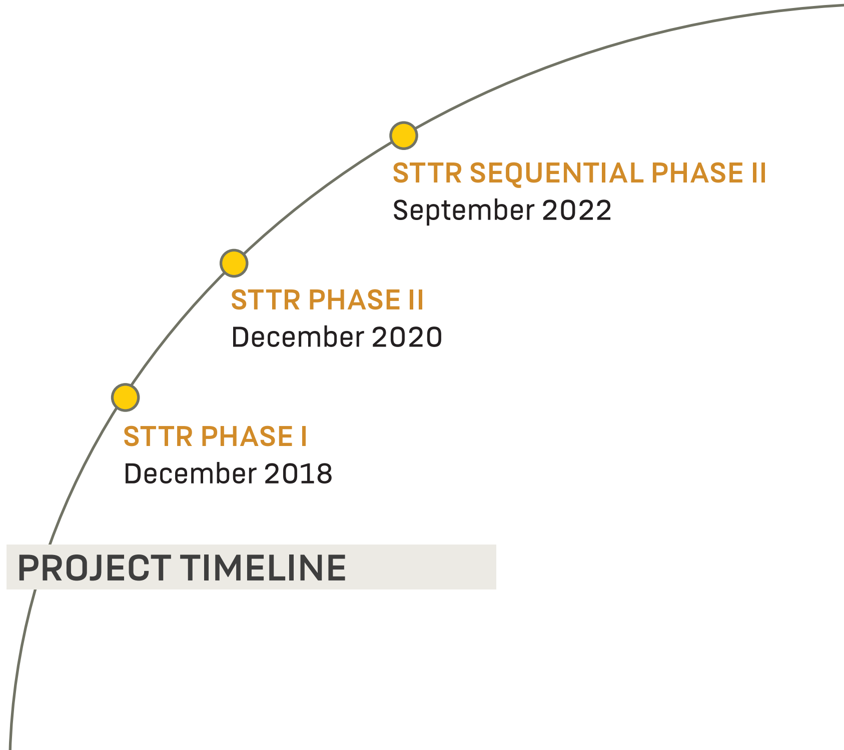
> "To meet the Army's modernization networking priority, we must ensure the Army's network is safe from malicious software. This new technology will allow cyber defenders to deal with malware especially ransomware effectively by identifying these threats and also having a reliable way to recover files locked up by adversaries should it happen."

Dr. Cliff Wang, Program manager
U.S. Army Combat Capabilities Development Command, Army Research Laboratory

"By the end of this program, we aim to have a beta-quality implementation, have completed field testing with prospective customers, and be positioned to pursue next steps in commercialization through a licensing arrangement or a spinoff," Siu said.
When Phase II is complete, the small businesses and their research partners are expected to obtain funding from a Department of Defense or Army system acquisition office and/or private sector, non-government sources to further develop the products in Phase III.

The Army STTR program invests in all Army modernization priorities via nine participating DEVCOM and Army science and technology centers.

Congress established the STTR program in 1992 to provide small businesses and research institutions with opportunities to participate in government-sponsored research and development.



PROJECT TIMELINE

STTR SEQUENTIAL PHASE II
September 2022

STTR PHASE II
December 2020

STTR PHASE I
December 2018