New cyberattack can trick scientists into making toxins or viruses

November 30 2020

Credit: Pixabay/CC0 Public Domain

An end-to-end cyber-biological attack, in which unwitting biologists may be tricked into generating dangerous toxins in their labs, has been discovered by Ben-Gurion University of the Negev cyber-researchers.

According to a new paper just published in *Nature Biotechnology*, it is

currently believed that a criminal needs to have physical contact with a dangerous substance to produce and deliver it. However, malware could easily replace a short sub-string of the DNA on a bioengineer's computer so that they unintentionally create a toxin producing sequence.

"To regulate both intentional and unintentional generation of dangerous substances, most synthetic gene providers screen DNA orders, which is currently the most effective line of defense against such attacks," says Rami Puzis, head of the BGU Complex Networks Analysis Lab, a member of the Department of Software and Information Systems Engineering and Cyber@BGU. California was the first state in 2020 to introduce gene purchase regulation legislation.

"However, outside the state, bioterrorists can buy dangerous DNA, from companies that do not screen the orders," Puzis says. "Unfortunately, the screening guidelines have not been adapted to reflect recent developments in synthetic biology and cyberwarfare."

A weakness in the U.S. Department of Health and Human Services (HHS) guidance for DNA providers allows screening protocols to be circumvented using a generic obfuscation procedure which makes it difficult for the screening software to detect the toxin producing DNA. "Using this technique, our experiments revealed that that 16 out of 50 obfuscated DNA samples were not detected when screened according to the 'best-match' HHS guidelines," Puzis says.

The researchers also found that accessibility and automation of the synthetic gene engineering workflow, combined with insufficient cybersecurity controls, allow malware to interfere with biological processes within the victim's lab, closing the loop with the possibility of an exploit written into a DNA molecule.

The DNA injection attack demonstrates a significant new threat of

malicious code altering biological processes. Although simpler attacks that may harm biological experiments exist, we've chosen to demonstrate a scenario that makes use of multiple weaknesses at three levels of the bioengineering workflow: software, biosecurity screening, and biological protocols. This scenario highlights the opportunities for applying cybersecurity know-how in new contexts such as biosecurity and gene coding.

"This attack scenario underscores the need to harden the synthetic DNA supply chain with protections against cyber-biological threats," Puzis says. "To address these threats, we propose an improved screening algorithm that takes into account in vivo gene editing. We hope this paper sets the stage for robust, adversary resilient DNA sequence screening and cybersecurity-hardened synthetic gene production services when biosecurity screening will be enforced by local regulations worldwide.

More information: Rami Puzis et al, Increased cyber-biosecurity for DNA synthesis, *Nature Biotechnology* (2020). DOI: 10.1038/s41587-020-00761-y

Provided by American Associates, Ben-Gurion University of the Negev