SUPPLY CHAINS

Research: How Malware Weaponized DNA

By Bruce Sussman

Read more about the author

TUE | DEC 7, 2021 | 10:53 AM PST

It's like the SolarWinds supply chain attack—except it involves the building blocks of life: DNA.

And it has the potential to secretly turn a therapeutic that could help you into something toxic that could harm you.

Researchers from Yale University in the U.S. and Ben-Gurion University in Israel just proved this type of attack can be successfully carried out.

Synthetic DNA industry: low hanging fruit for cyberattack

The synthetic biology industry is worth billions, and forecast to top the $20 billion mark in the next few years.

A crucial part of this industry is the creation and sale of synthetic DNA. This type of material is both complicated

Most Recent

and useful. And synthetic DNA plays a part in lots of research, including in the development of new therapeutics and vaccines. Another example comes from agriculture, where it has helped increase crop yields.

However, new research says the cybersecurity of this supply chain is unprepared to withstand cyberattacks that could secretly make synthetic DNA some sort of biological weapon.

It's another example of the cyber world putting the real world at risk.

Proof of concept: attacking the synthetic DNA supply chain

In the case of the SolarWinds cyberattack, threat actors secretly placed malicious code inside the company's legitimate software updates.

SolarWinds customers around the globe, and their IT networks, welcomed the updates inside as legitimate code. Everything technically checked out and was verified as authentic; however, malicious code was obfuscated—hidden inside.

Researchers from Yale and Ben-Gurion universities just carried out a similar style of cyberattack involving synthetic DNA.

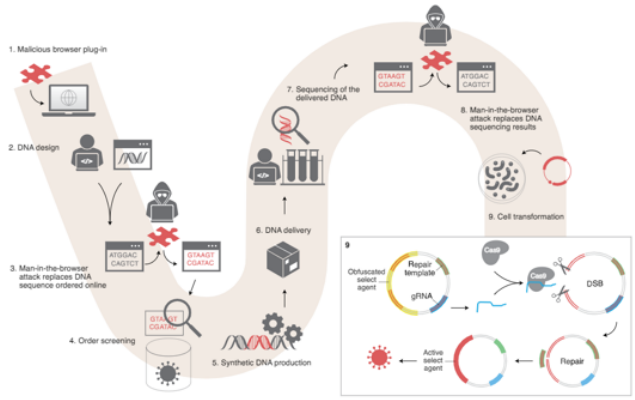
Here is a note from their attack summary, which they published in *Nature*:

> "This threat is real. We conducted a proof of concept: an obfuscated DNA encoding a toxic peptide was not detected by software implementing the screening guidelines. The respective order was moved to production. Details are withheld, but IGSC was notified about the threat and potential mitigation methods. The order was canceled for biosecurity reasons following our disclosure."

In simple terms, this means they made some legitimate

synthetic DNA toxic on the inside and nothing caught it. Like that SolarWinds code, the DNA code was legitimate on the outside but held something dangerous within.

Here is a look at how the attack can be carried out:



There is a lot going on here, but follow the items in red.

At the start, the first piece of the puzzle is malware that compromises a scientist's device. That compromise ripples through the entire DNA development process, and this eventually weaponizes the output which is represented at the end by that red cell that looks like a spike protein.

Here's an illustration from their research:

> "Eve is a cyber-criminal targeting Alice. Eve can easily infect Alice's vulnerable computers with malware. Eve replaces all or part of Alice's order with a malicious sequence (Fig. 1).
>
> Eve employs DNA obfuscation—inspired by cyber-hacking malicious code obfuscation—to camouflage fragments of the pathogenic DNA in the hijacked order. Bob will not detect the malicious DNA; with obfuscation, best-match-based screening procedures will return legitimate matches...."

In other words: current screening methods will give this altered DNA a green light.

> "Bob's delivered product includes a sequencing report showing the DNA as error-free. Alice may seek additional confirmation, but malware will ensure that the results will falsely reflect the original DNA sequence that Alice intended to order (Fig. 1)."

And then that malicious DNA can be produced, sold, and used in something that may end up inside humans.

How do we defend against cyberattacks on biosciences?

How can researchers, scientists, and bioscience companies mitigate the risk and make this supply chain more resilient?

The researchers, in this case, say everyone involved needs to focus more on "cyber-biosecurity," which is the convergence of biosecurity and cybersecurity.

Here are four things the security researchers suggest for the biosciences industry:

1. "Synthesizers can implement cybersecurity protocols, such as electronic signatures on orders, and adapt to provide intrusion detection approaches, ranging from heuristic signatures to artificial intelligence behavioral analysis, to identify malicious code."
2. "The current 200-bp screening windows should be reduced to the length of the shortest homology-directed repair template required for deobfuscation."
3. "Fulfilled orders should be revisited when new information arises."
4. "Data should be shared (in a privacy-preserving manner) to enable detection of malicious orders deliberately distributed across multiple synthesizers."

Researchers are also calling for more legislation and

regulation as a way of moving things forward. Could this be something for the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to explore? We'll see.

In the meantime, this is another example of cyber convergence:

> "Cyber dangers are spilling over to the physical space, blurring the separation between the digital world and the real world, especially with increasing levels of automation in the biological lab. Best practices and standards must be woven into operational biological protocols to combat these threats."

Resources

See the latest SecureWorld cybersecurity conference calendar

Podcast: Nation-State Cyber Threats: What Now?

SECUREWORLD SESSIONS
Nation-State Cyber Threats: What Now?

Tags: Supply Chains, Malware

Comments

First Name*

Last Name

Email*

Comment*

protected by reCAPTCHA
Privacy - Terms

Submit Comment

See what SecureWorld can do for you. Contact us today! CONTACT US

First name*

Email address*

SUBSCRIBE