DNA Testing Kits & The Security Risks in Digitized DNA

By
Candice Lanier (https://www.bleepingcomputer.com/author/candice-lanier/)

December 7, 2018 10:43 AM **0**

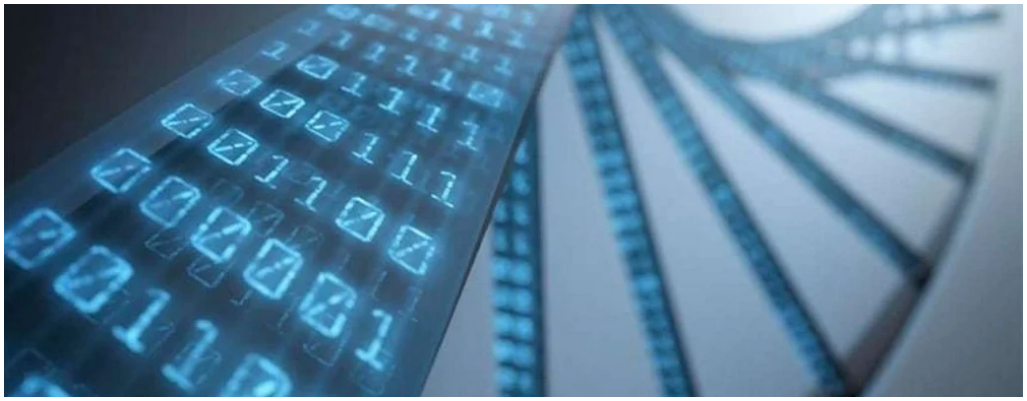

Photo Credit: Huffington Post

Direct-to-consumer DNA testing services have experienced a surge in popularity over the past few years. Digitizing DNA (https://www.forbes.com/sites/forbestechcouncil/2018/11/29/hacking-humans-protecting-our-dna-from-cybercriminals/#50abde1e5287) carries the benefits of uncovering ancestry information and can have significant positive impact on science and medical research. It can, for instance, assist in finding a cure for a fatal disease.

Cyberbiosecurity

According to Peccoud Lab, which specializes in synthetic biology informatics at Colorado State University, Cyberbiosecurity (https://www.peccoud.org/synthetic-biology-informatics/cyberbiosecurity-biological-security/) is a specialty that deals with understanding and mitigating new biological security risks emerging

at the interface between biosecurity and cybersecurity. The digitization of DNA involves its storage in a database. The solving of a criminal cold case through matching a consumer DNA database with a police database is another example of how digitized DNA can be used.

The Risks

The addition of digitized DNA provides hackers with another target to exploit and opens up a new and challenging frontier for cybersecurity professionals. There are significant implications (https://www.techrepublic.com/article/how-to-manage-cyberbiosecurity-risks-before-a-malware-attack-strikes/) involved in digitizing DNA.

"The cyber-physical nature of biotechnology raises unprecedented security concerns," coauthors Jean Peccoud, Jenna E. Gallegos, Randall Murch, Wallace G. Buchholz, and Sanjay Raman explain in their research paper titled, Cyberbiosecurity: From Naive Trust to Risk Awareness. "Computers can be compromised by encoding malware in DNA sequences, and biological threats can be synthesized using publicly available data."

Potential security risks include:

- Digital representations of genes could be used to make biologic weapons (https://www.incsnow.com/cyberbiosecurity-computers-make-malicious-modification-of-dna-as-easy-as-editing-text/).
- Because vulnerabilities exist in computers, hackers could compromise a device, with the intent to stall the production of critical drugs, for example. This could be accomplished by using a methodology similar to that which was used with Stuxnet.
- The Centers for Disease Control (CDC) have already successfully used published DNA sequences as a prototype to reconstruct the virus responsible for the Spanish flu, which was one of the deadliest pandemics ever.
- Scientists in Israel have shown that it is possible to fabricate (https://www.nytimes.com/2009/08/18/science/18dna.html) DNA evidence. These scientists “fabricated blood and saliva samples containing DNA from a person other than the donor of the blood and saliva. They also showed that if they had access to a DNA profile in a database, they could construct a sample of DNA to match that profile without obtaining any tissue from that person.”
- Giovanni Vigna, professor of computer science at University of California Santa Barbara and co-founder of Lastline, has suggested that hackers might start selling DNA data back for ransom (https://www.theverge.com/2018/6/6/17435166/myheritage-dna-breach-genetic-privacy-bioethics).

- Hackers could also threaten to “revoke access (https://www.theverge.com/2018/6/6/17435166/myheritage-dna-breach-genetic-privacy-bioethics) or post the sensitive information online if not given money; one Indiana hospital paid $55,000 to hackers for this very reason.”
- There are other reasons why genetic data could be lucrative (https://www.theverge.com/2018/6/6/17435166/myheritage-dna-breach-genetic-privacy-bioethics). “This data could be sold on the down-low or monetized to insurance companies,” Vigna cautions. “You can imagine the consequences: One day, I might apply for a long-term loan and get rejected because deep in the corporate system, there is data that I am very likely to get Alzheimer’s and die before I would repay the loan.”
- Stolen DNA (https://itknowledgeexchange.techtarget.com/storage-disaster-recovery/what-could-you-do-with-a-stolen-dna-database/) could be planted in order to incriminate someone.
- It could be used to receive or deny medical treatment.
- It could be used (https://itknowledgeexchange.techtarget.com/storage-disaster-recovery/what-could-you-do-with-a-stolen-dna-database/) to mask a genetic condition, in the same way people will purchase clean urine so they can pass a drug test.
- Security researchers were able to infect a computer (http://dnasec.cs.washington.edu/#our-team) with malware embedded in a strand of human DNA.

Peccoud and Gallegos write (https://www.incsnow.com/cyberbiosecurity-computers-make-malicious-modification-of-dna-as-easy-as-editing-text/) that, "With the help of computers, editing and writing DNA sequences are almost as easy as manipulating text documents. And it can be done with malicious intent." Rashmi Knowles (https://www.cbronline.com/news/myheritage-hack), EMEA Field CTO at RSA Security has commented that, “many people don’t think about this when applying for such services. No matter how secure the organization, no one is completely risk-free, and if breached, genetic data could be sold on hackers without your consent, or the characteristic data it contains could be used to hijack your online accounts.”

DNA Testing Kits

According to The Verge (https://www.theverge.com/2018/6/6/17435166/myheritage-dna-breach-genetic-privacy-bioethics):

> "MyHeritage doesn't offer health or medical tests, but many companies, like 23andMe and Helix, do. And there are plenty of players interested in DNA: researchers want genetic data for scientific studies, insurance companies want genetic data to help them calculate the cost of health and life insurance, and police want genetic data to help them track down criminals, like in the recent Golden State Killer case. Already, we lack robust protections when it comes to genetic privacy, and so a genetic data breach could be a nightmare. "If there is data that exists, there is a way for it to be exploited," says Natalie Ram, a professor of law focusing on bioethics issues at the University of Baltimore.
>
> Genetic testing sites are treasure troves of sensitive information. Some sites offer users the option to download a copy of their full genetic code while others don't. But the full genetic code isn't the most valuable information anyway. As Ram points out, we can't just read genetic code like a book to gain insights. Instead, it's the easy-to-access account pages with health interpretations that are most useful for hackers."

Risky across the board

Then too, there is forensic use of genetic databases, such as the FBI's DNA Index System (CODIS) and the public genealogy database GEDmatch, both of which were described by Science Magazine (http://www.sciencemagazinedigital.org/sciencemagazine/23_november_2018/MobilePagedArticle.action?articleId=1443800&app=false#articleId1443800) as "nothing less than "haphazard and underregulated."

Researchers at the Center for the Study of Weapons of Mass Destruction at the National Defense University point out that both researchers and bio-industrial companies store and use genomic data on computers, local area networks and/or cloud services and transfer the data between users over email or other sharing technologies. Hence, it is "exposed (https://www.hsdl.org/?view&did=813127) at many touch points throughout their use to the risks and vulnerabilities common to cyberspace such as hacking, data theft, sabotage, and unauthorized access. In most cases, only minimal encryption or other cybersecurity safeguards are used to secure genomic data at these touch points in the information life cycle."

The researchers go on to warn that these risks are exacerbated by an overall lack of awareness among scientists and researchers, in addition to the need for effective measures for protecting genomic data in the first place. They also argue that the securing of genomic data should not be

viewed merely as a subset of cybersecurity, because safeguarding of genomic data necessitates an understanding of how bio-scientists use and could potentially misuse such information.

Related Articles:

Estonia arrests hacker who stole 286K ID scans from govt database (https://www.bleepingcomputer.com/news/security/estonia-arrests-hacker-who-stole-286k-id-scans-from-govt-database/)

DNA (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/DNA/)

PRIVACY RISK (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PRIVACY-RISK/)

TESTING KIT (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/TESTING-KIT/)

(https://www.bleepingcomputer.com/author/candice-lanier/)

CANDICE LANIER (HTTPS://WWW.BLEEPINGCOMPUTER.COM/AUTHOR/CANDICE-LANIER/)
(MAILTO:INFO@GHOSTCYBERINTEL.COM) (HTTPS://TWITTER.COM/CANDICELANIER)

Chief Operations Officer at CyberSec Express (CSE), a provider of managed cybersecurity. CSE is in the process of launching a nonprofit for low-income children to receive free computers and cybersecurity training. Educational background is in criminology, psychology, computer science and digital forensics. In addition to Bleeping Computer, I also write for Security Affairs, was featured on an episode of VICELAND's Cyberwar and on EFF.Org.

PREVIOUS ARTICLE

(HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/DNA-TESTING-KITS-AND-THE-SECURITY-RISKS-IN-DIGITIZED-DNA/)

NEXT ARTICLE

(HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/DANABOT-BANKING-TROJAN-GETS-INTO-CRAM-BUSINESS/)