FTI CONSULTING | CYBERSECURITY

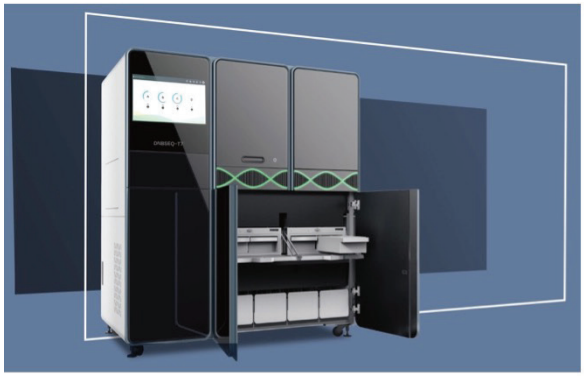
Complete GENOMICS

FTI Consulting Data Security Assessment: Complete Genomics' U.S. Customer Offering

Published October 18, 2023

SUMMARY:

FTI Consulting, Inc. ("FTI") was engaged by Complete Genomics ("Client" or "CG") to conduct network monitoring, vulnerability assessments, and hardware and source code review pertaining to its DNBSEQ-T7 product ("T7"), sold to US customers as a package that additionally includes a separate Linux based Server ("ZTRON Lite" or "ZTRON") used for storing, processing, and transmitting genomic sequencing data produced by the T7, between August 30, 2023 and October 16, 2023.[1] This assessment sought to identify the existence and nature of any outbound network traffic occurring during US customers' expected DNA sequencing operations while using the T7 and ZTRON.



KEY FINDINGS:

1. NETWORK CAPTURE:

- During the assessment period, live network captures from the ZTRON server revealed external Internet Protocol (IP) activity and traffic attributable to known Linux repositories, Domain Name System (DNS), and Network Time Protocol (NTP) servers (collectively "system functionality IPs") which were all based in the United States of America and considered expected traffic.
- Further analysis of the system functionality IPs at the time of the assessment revealed **no meaningful data transfer in the outbound traffic.**

2. SOFTWARE SOURCE CODE REVIEW:

- Results from review of limited2 ZTRON source code, made available at the time of the assesment, indicated that the domain name "ztron.mgitech.com" is hardcoded within the code for the apparent purpose to access and transfer data.
- According to information from CG, **this functionality is intended for the global version of the ZTRON's operating system only.**
- This statement **is consistent with FTI's observations** that the ZTRON's US version operating system did not appear to invoke this functionality, as the IP address corresponding to that domain did not appear in network captures performed during the assessment period.

3. VULNERABILITY SCANS:

FTI does not have immediate reason to believe that any of the vulnerabilities identified during the period of assessment:

- Pose a significant threat to the legitimacy or efficacy of FTI's testing procedures;
- Have any connection to the external IP connections that were made during regular operations of the systems;
- Pose an apparent threat to the security of the ZTRON as delivered to US clients.

4. HARDWARE SCHEMATIC REVIEW:

Based on the product schematics and information made available by CG at the time of the assessment:

- FTI **identified no inconsistencies in the hardware** schematic design, design rules, schematic conventions, and documentation related to the ZTRON.
- FTI assesses the CG-provided schematic diagrams are of a high-quality design and engineering work product.

CONCLUSION:

FTI's approach revealed that, during the period of assessment and leveraging the requested materials provided by CG, the ZTRON and T7 functionality contained within CG's US version:

1. **Did not result in outbound, external IP communications** during genomic sequencing aside from that required for Linux system functionality;
2. **Did not contain immediately concerning source code or network vulnerabilities;**
3. Otherwise appeared **consistent with expected hardware design.**

[1] FTI notes that all network traffic was captured on CG configured devices and within a CG controlled environment. Additionally, all software repositories and resources were provided by CG under the assumption that it accurately reflects the live CG software repositories; the software environment that FTI accessed was fully controlled and managed by CG personnel.