HC3: Alert

November 23, 2021 TLP: White Report: 202111231300

BIO-ISAC Tardigrade Amplify Alert

Executive Summary

The cybersecurity nonprofit Bioeconomy Information Sharing and Analysis Center (BIO-ISAC) recently released research on a new strand of sophisticated malware that is aggressively spreading throughout the biomanufacturing industry. They labelled this malware Tardigrade and have released a report with their analysis and recommendations. Due to its "unprecedented sophistication and stealth", the researchers suspect an Advanced Persistent Threat (APT) is operating it. HC3 recommends that biotechnology companies specifically as well as the healthcare and public health sector (HPH) generally review this report and take appropriate action to protect their information infrastructure against the spread of Tardigrade.

Report

BIO-ISAC Releases Advisory to Biomanufacturers
https://www.isac.bio/post/tardigrade

Impact to HPH Sector

The researchers describe Tardigrade as highly sophisticated and aggressively spreading throughout the biomanufacturing sector. It's used to deliver ransomware, possibly as a diversion for the actual purpose of the attack – intellectual property theft. Tardigrade is described as unusually capable, able to customize its build depending on the victim environment, making detection challenging. It can recompile its loader from memory without leaving a consistent signature and is therefore classified as metamorphic. Tardigrade can operate autonomously when cut off from its operators. They also noted that Tardigrade resembles a popular loader known as Smoke Loader (also known as Dofoil). The researchers offer presentation slides and a video presentation (see link above). They also offer IOCs at their website, https://www.isac.bio/.

References

Devious 'Tardigrade' Malware Hits Biomanufacturing Facilities
https://www.wired.com/story/tardigrade-malware-biomanufacturing/

VirusTotal submission results
https://www.virustotal.com/gui/file/c0976a1fbc3dd938f1d2996a888d0b3a516b432a2c38d788831553d81e2f5858/detection

Tardigrade hackers target big pharma vaccine makers with stealthy malware
https://www.bleepingcomputer.com/news/security/tardigrade-hackers-target-big-pharma-vaccine-makers-with-stealthy-malware/

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback