THIRD-PARTY REPORT 2023

Nubeva Ransomware Reversal

Product Assessment by MISI

nubeva

About MISI

MISI is a cybersecurity nonprofit fueling the people and technology needed to solve critical cybersecurity challenges. MISI's three pillars of focus include: small business and academic engagement, STEM and workforce development, and proof of concept innovation. Through collaboration with small businesses, academic researchers, and non-traditional members of the cybersecurity community, MISI serves as an intermediary and helps connect U.S. Cyber Command (USCYBERCOM) and the U.S. government to the innovative products and solutions needed to advance the nation's cybersecurity capabilities.

MISI operates programs out of MISI facilities, including two nationally acclaimed Cyber Mission Accelerators with over 100,000 square feet of space: DreamPort and MindScape. DreamPort was created in partnership with US Cyber Command (USCYBERCOM) as a non-government-owned or operated independent facility to provide cyber national mission forces and partners with continuous innovation in cyber capabilities.

Visit https://misi.tech/ to learn more.

For permissions or inquiries regarding the use of this report, please contact:
Nubeva Inc.
Email: info@nubeva.com
Website: www.nubeva.com

Executive Summary

This report contains the final results of the test and evaluation of the Nubeva Ransomware Reversal (NuRR) platform from Nubeva Inc. NuRR claims the ability to decrypt ransomed data as a means to recovery of ransomed data from a successful ransomware attack. The purpose of this effort is to test those claims and the overall solution platform. The MISI engineers conducting this test have twenty-five (25) years of experience in malware analysis and reverse engineering. This effort took place between 01 May and 31 May 2023

Outcome

There are seventeen (17) procedures defined in the associated test plan for this platform. TESTER offers the following bottom line up front (BLUF) of these results:

- Of the seventeen (17) tests conducted, there were 17 successful pass(es)
- There were zero (0) recorded test failures.

1. NuRR Captures Keys

Results provide sufficient evidence for VENDOR to state **Nubeva key capture rate was 100%** from tested ransomware including Lockbit, Ragnar Locker, BlackBasta and several others that represent a significant percentage of real-world attacks.

2. NuRR Decrypts

Decryption was demonstrated using captured keys validating the keys and the full product capability and value lifecycle.

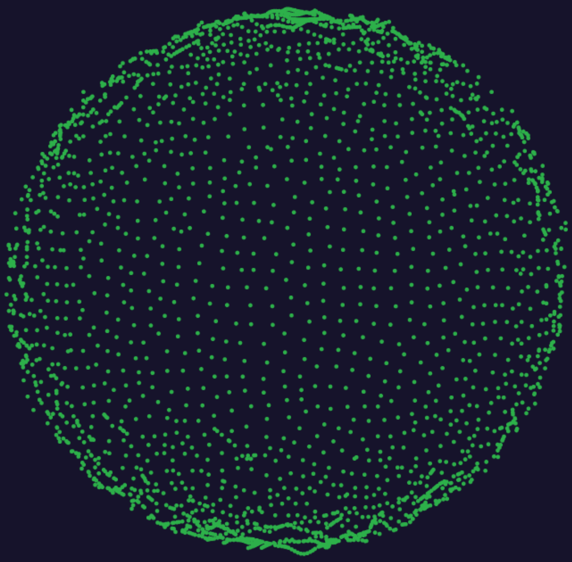
3. NuRR's Overall System Is Simple and Secure

- VENDOR automation deploys using cloud components that are easy to set up, easy to operate, and provide for significant customizations and integrations.
- Azure cloud backend (as tested) was trivial to implement and use for a junior engineer
- ***Endpoint agent did not introduce observed system instabilities during test.***
- ***NURR does not open network ports or introduce vulnerabilities into an endpoint as measured by nmap and BitDefender Total Security***
- The specific architecture tested (as described in section titled Vendor Architecture) including Azure cloud services and host agent uses secure best practices.

Opinion

MISI is excited about this product and believe it shows real promise. Decryption is arguably one of the fastest and lowest data-loss means to recover data from a ransomware attack, and as such, represents a new potential layer of defense. Given these testing results and the simplicity of the NuRR decryption solution, we feel NuRR represents a very real potential safety-net for many organizations to consider. We hope to see NuRR successful in helping its customers recover from future ransomware infections where this platform has been installed.

MISI hopes Nubeva continues to push its capabilities forward and welcomes further expanded testing of the product to aid in continued improvements.



misi

www.misi.tech

Full Report Available to Validated Customers, Prospects, and Partners

www.nubeva.com - info@nubeva.com

REQUEST ACCESS