TAG

SAFEGUARDING DATA FROM ADVANCED CYBER THREATS USING CYBERVORE

DR. EDWARD AMOROSO, CEO, TAG,
RESEARCH PROFESSOR, NYU

CARLIER HERNANDEZ,
RESEARCH ASSOCIATE, TAG DATA RESEARCH TEAM

Cybervore™

SAFEGUARDING DATA FROM ADVANCED CYBER THREATS USING CYBERVORE

DR. EDWARD AMOROSO, CEO, TAG[1], RESEARCH PROFESSOR, NYU
CARLIER HERNANDEZ, RESEARCH ASSOCIATE, TAG DATA RESEARCH TEAM

INTRODUCTION:

Our analyst and research team at TAG recently became aware of a New Jersey-based cybersecurity startup company called Cybervore.[2] The company provides an interesting product called Fragglestorm that safeguards user data against sophisticated cyber-attacks, up to and including threats from quantum computing. The product achieved this objective through a unique combination of encryption and fragmentation techniques.

This report provides an independent analysis of Cybervore and its flagship offering. Our goal is to provide insight into how the solution works, where it will best serve customers, and how it will stack up against common threats. Our hope is that this information will help potential buyers and investors better understand the specifics of this new company and its mission to reduce data risk.

OVERVIEW OF FRAGGLESTORM

What drew us to Cybervore is that their Fragglestorm product goes about the task of data protection in a manner that is different than we see for most traditional products. The most common methods we see from current vendors will rely mostly on data encryption. While this is certainly essential – and it is a major component of the Cybervore solution, it is usually also not sufficient to handle a determined adversary.

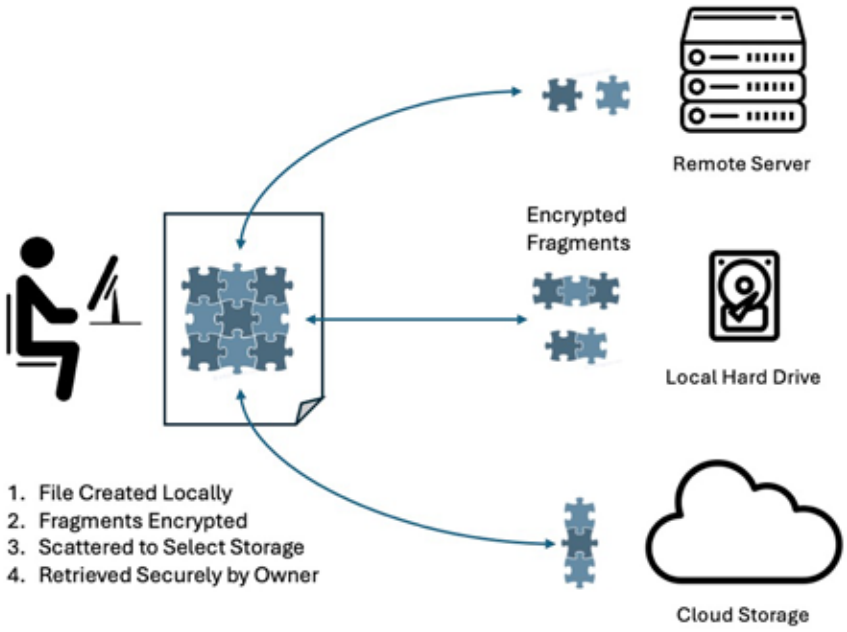

Figure 1. Fragglestorm Storage of Fragments

Fragglestorm specifically enhances data security by integrating encryption (i.e., using the Advanced Encryption Standard (AES)) with a proprietary fragmentation process, resulting in data being transformed into unrecognizable encrypted fragments scattered across various storage options. This layered approach ensures that even if data is intercepted or accessed without authorization, it remains indecipherable and useless to malicious actors.

In the section below, we will try to explain this process, including how it is implemented using a virtual drive that makes the underlying security mostly invisible to users. As one would expect, for users with high risk, but perhaps low tolerance, patience, or even skill level for cybersecurity (e.g., law firms, medical groups), the use of a desktop data security solution that is easy to use seems a mandatory requirement.

HOW FRAGGLESTORM WORKS

The core component of Fragglestorm is referred to as the Fraggledrive, which is a software-based virtual drive that operates within a user's existing system environment. It is designed to look pretty normal to users who create, manage, and try to secure important files on their PC. In order to understand how the Cybervore product works, it will help to go through each of the components of how Fraggledrive operates:

VIRTUAL DRIVE INTEGRATION

Fraggledrive integrates into a user's computer by installing itself as an additional disk drive, offering a familiar and intuitive interface without necessitating extra hardware. This design ensures that users can interact with their files as they normally would, while Fraggledrive operates transparently in the background to provide robust security measures. The install process is straightforward using a well-documented guide and set-up wizard.

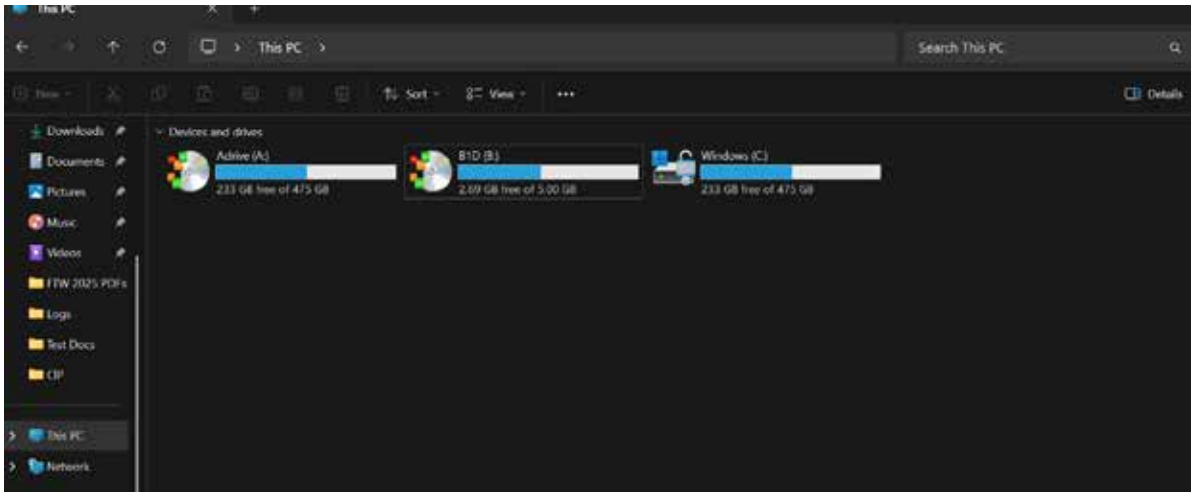

Figure 2. Sample View of Drives Set Up Using Fragglestorm

USER AUTHENTICATION

Access to Fraggledrive is strictly limited to authorized users, ensuring that sensitive data remains protected even if the physical device is compromised. This stringent access control aligns with zero-trust security principles, allowing only authenticated individuals to activate and utilize the drive. This is done through Okta/Auth0 and generally involves downloading an app called Guardian to the smartphone to complete the authentication process.

REAL-TIME ENCRYPTION AND FRAGMENTATION

Upon saving data to Fraggledrive, the information is immediately encrypted using robust standards and fragmented into unrecognizable pieces. This dual-layered approach converts data into puzzle-like fragments, rendering it useless to unauthorized users and significantly enhancing security.

DISTRIBUTED STORAGE

The fragmented data pieces are unevenly distributed across user-designated storage locations, which may include on-premises devices, multiple cloud services, or a hybrid combination. This strategic dispersion ensures that no single storage location contains the complete dataset, adding an additional layer of security and resilience against breaches. Our view is that this layer of protection is attractive for particularly sensitive files (e.g., legal documents, health records).

FLEXIBLE STORAGE OPTIONS

Each Fraggledrive supports up to 64 consumer and commercial cloud services and on-premises networked devices, providing users with extensive flexibility in managing their data storage strategies. This versatility allows for tailored solutions that can adapt to various organizational needs and compliance requirements. The Fragglestorm interface allows for adding and managing different data sources (drives appear in the File Explorer like other local storage).

CONTROLLED ACCESSIBILITY

Users have the ability to manually or automatically deactivate Fraggledrive, effectively removing data accessibility when not in use. This feature is particularly beneficial in preventing unauthorized access during periods of inactivity, ensuring that sensitive information remains secure at all times.

BENEFITS OF USING FRAGGLESTORM

Implementing Fragglestorm offers numerous advantages that address both current and emerging cybersecurity challenges:

Enhanced Data Security: The combination of encryption and fragmentation creates a formidable barrier against unauthorized access, rendering stolen data unreadable and unusable.
Augmentation of Existing Security Measures: Fragglestorm complements and strengthens existing cybersecurity investments, contributing to a comprehensive defense-in-depth strategy.
Integration: Designed for user-friendliness, Fragglestorm integrates transparently with existing applications and workflows, minimizing disruption and eliminating the need for extensive retraining.
Strict Access Control: Built-in identity access management services ensure that only authorized users can activate and access their protected data, enhancing overall security posture.
Flexible Compliance Management: Users can designate storage locations to meet specific compliance, governance, and regulatory requirements, providing greater control over data management practices.

Interestingly, the Cybervore team is anticipating quantum threats coming soon with future advancements in quantum computing. Fragglestorm is thus engineered to provide robust protection against emerging quantum threats. Our view is that most users will not be concerned with this threat today, but we agree that the problem will emerge in the coming years and decades.

CONCLUSION

Based on our review of the platform, including installing and testing is use, we can confidently conclude that Cybervore's Fragglestorm offers an effective approach to multi-layered data protection. By tangling encryption with fragmentation and distributed storage techniques, Fragglestorm provides Windows PC users with a robust, flexible, and user-friendly solution to safeguard files.

Readers interested in more information about Cybervore, or other related areas of cybersecurity are encouraged to reach out to the TAG team for guidance. TAG Research-as-a-Service (RaaS) customer can connect through their RaaS portal account. Readers are also encouraged to reach out directly to the Cybervore team for additional information on the Fragglestorm product including pricing information.

---

[1] Founded in 2016, New York-based TAG Infosphere provides research and advisory in cybersecurity and AI for enterprise, government, researchers, and vendors. This report is part of a series of in-depth analyses of security vendors for TAG Research as a Service (RaaS) customers. The material is presented for informational purposes and not intended to guide personal investment (see https://www.tag-infosphere.com/).

[2] Cybervore's management and leadership team is comprised of seasoned professionals with extensive experience in technology and financial services (see https://www.cybervore.com/).

ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity and artificial intelligence,.