LUCRATIVE RANSOMWARE ATTACKS: ANALYSIS OF THE CRYPTOWALL VERSION 3 THREAT

CYBER THREAT ALLIANCE

EXECUTIVE SUMMARY

The Cyber Threat Alliance (CTA) is a group of leading cybersecurity solution providers who have joined together to share threat intelligence on advanced attacks, their motivations, and the tactics of the malicious actors behind them. Members of the CTA use this intelligence to improve the collective defense offered to their respective customers, protecting them from threats observed and shared across all members.

In order to improve the security posture of the entire community, the Cyber Threat Alliance conducted in-depth research into CryptoWall, one of the most lucrative and broad-reaching ransomware campaigns affecting Internet users today. Sharing intelligence and analysis resources, the CTA profiled the latest version of CryptoWall, which impacted hundreds of thousands of users, resulting in over US $325 million in damages worldwide.

WHAT IS RANSOMWARE?

Ransomware is a type of malware that encrypts a victim's files and subsequently demands payment in return for the key that can decrypt said files. These files may contain various types of information, such as important financial data, business records, databases, and personal files that may hold sentimental value to the victim, such as photos and home movies. Once these files are identified, the malware will encrypt them using a key known only by the attackers. In order to acquire this key to decrypt these files, the victim must pay a ransom to the attackers, often in the form of electronic currency, such as bitcoin.

The Cyber Threat Alliance examined the full attack lifecycle of the CryptoWall v3 threat, crafting a comprehensive research paper analyzing the propagation, malware, campaign details, command-and-control infrastructure, and financial impact.

Highlights from the report include:

- **An estimated US $325 million in damages**
- **406,887 attempted infections of CW3**
- **4,046 malware samples**
- **839 command and control URLs**
- **Practical recommendations for mitigating and preventing the threat.**

Readers are encouraged to use the data provided in this report to better protect themselves and can use any intelligence in it freely, including:

- Scripts and files provided on the Cyber Threat Alliance GitHub **repository.**
- CryptoWall **tracking dashboard,** providing the latest CW3 samples and C2 URLs.

Beyond this public sharing of intelligence, the threats, tactics, and indicators covered within this report have been shared with all Alliance members to maximize protection for their respective customers.

Download the Full Report