SEQRITE

DarkRace Ransomware

is a derivative of the infamous Lockbit ransomware, incorporating heavily from its leaked source code.

A deep dive into its techniques and impact

www.seqrite.com

SEQRITE

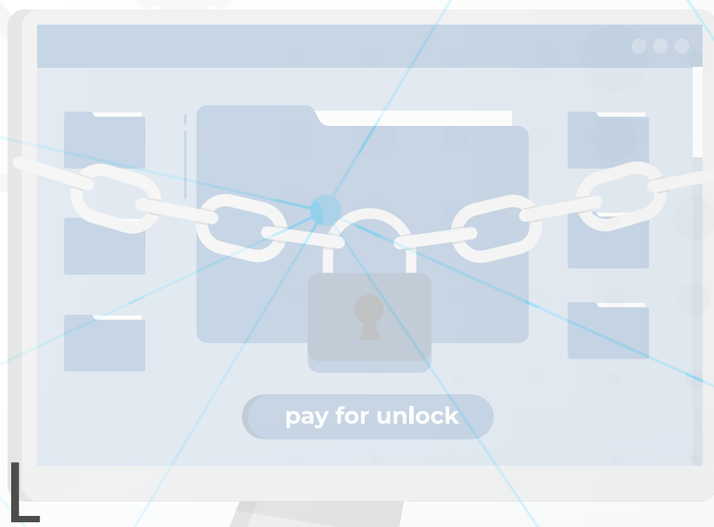
How does it spread?

Cracked Software Infiltration :
The ransomware discreetly enters systems through cracked software installations using obfuscator technology.

Phishing Email Attacks :
DarkRace employs social engineering in phishing emails, deceiving users into activating exploit kits and initiating ransomware attacks.

SEQRITE

Characteristics and Tactics used by DarkRace



1. **Runtime Decryption:** DarkRace ransomware dynamically decrypts XML data during runtime, revealing crucial information for adaptability and complicating countermeasures.

2. **Encryption using Salsa20:**
DarkRace employs the Salsa20 stream cipher for fast and secure file encryption, appending random extensions to hinder access until a ransom is paid.

3. **Post Encryption Measures:**
DarkRace deletes shadow copies, terminates interfering processes, deletes its own files, and restarts the system, intensifying the challenge for cybersecurity experts to trace its activities and develop countermeasures.

Criticality: High

Sectors Targeted:

Manufacturing, Financial, Transportation, Science & Technology

Regions: Europe and The United States

Unlock More Insights

Download The India Cyber Threat Report 2023

www.seqrite.com