ANY.RUN Uncovers New PE32 Ransomware Targeting Businesses with Double Extortion

DUBAI, DUBAI, UNITED ARAB EMIRATES, April 22, 2025 /EINPresswire.com/ -- ANY.RUN, a leading provider of interactive malware analysis and threat intelligence services, has released a new report by Mauro Eldritch detailing the emerging PE32 Ransomware, a rapidly spreading threat that poses significant risks to organizations across industries.

□□□□ □□□□□□□□□□: □ □□□□□□□□ □□□□□□□ □□ □□□□□□□□□□ □□□□□□□□□

PE32's ability to encrypt critical files and exfiltrate data threatens organizations in banking, retail, healthcare, manufacturing, and technology. Some of its key functionalities include:

· Rapid File Encryption: PE32 targets visible folders like the Desktop, appending a .pe32s extension, and begins encryption after minimal user interaction.

· Dual Ransom Demands: Unlike typical ransomware, PE32 employs a two-tier payment model: $700 to $7,000 for file decryption and $10,000 to 2 BTC for preventing data leaks.

· Telegram-Based Command and Control (C2): The ransomware uses the Telegram Bot API for communication, with exposed bot tokens making it traceable but no less disruptive.

Its lack of obfuscation and reliance on basic Windows libraries highlight inexperienced authors behind the threat, yet its active development signals growing danger.

Read detailed analysis of this ransomware strain on ANY.RUN's blog.

□□□ □□□.□□□ □□□□□ □□□□□□□□□ □□□□□□ □□□ □□□□□□□ □□□□

Using ANY.RUN’s Interactive Sandbox, organizations can analyze PE32 Ransomware in a secure, cloud-based environment. The service simplifies extraction of Indicators of Compromise (IOCs), monitors Telegram-based C2 activity, and maps attack behaviors, enabling faster response and recovery.

□□□□□ □□□.□□□

ANY.RUN empowers organizations in banking, manufacturing, telecommunications, healthcare, retail, and technology with cutting-edge malware analysis and threat intelligence. Its cloud-based Interactive Sandbox, paired with advanced tools like TI Lookup and YARA Search, helps businesses analyze threats in under 40 seconds, building resilient cybersecurity operations.

The ANY.RUN team
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:
X
YouTube
