Subject: RedEnergy Stealer: A New Ransomware Threat to the Energy and Telecom Sectors
Posted by admin on Thu, 30 Jul 2026 07:55:49 GMT
View Forum Message <> Reply to Message

RedEnergy Stealer: A New Ransomware Threat to the Energy and Telecom Sectors

"Beware of the New RedEnergy Ransomware That's Targeting Energy and Telecom Companies"

Meta Description: New RedEnergy Ransomware Targets Energy and Telecom Companies, Stealing Sensitive Data and Encrypting Files

linkedin-threat

Jul 7, 2023

A new ransomware threat dubbed RedEnergy has been spotted in the wild targeting energy utilities, oil, gas, telecom, and machinery sectors in Brazil and the Philippines through their LinkedIn pages.

The malware, which is not to be confused with the Australian company Red Energy, is a stealer-as-a-ransomware (StAR) threat. This means that it is designed to steal sensitive data from its victims before encrypting their files.
How RedEnergy Works

RedEnergy is distributed through fake browser update campaigns. Once it is installed on a system, it will steal information from a variety of sources, including:

- Web browsers (Chrome, Firefox, Edge, Opera)
- Email clients (Outlook, Thunderbird)
- Password managers (LastPass, 1Password)
- Crypto wallets
- File-sharing services (Dropbox, Google Drive)

After stealing this data, RedEnergy will encrypt the victim's files using the AES-256 encryption algorithm. The encrypted files will be suffixed with the ".FACKOFF!" extension.

The attackers then demand a ransom of 0.005 BTC (about $151) in exchange for the decryption key.
How to Protect Yourself from RedEnergy

There are a few things you can do to protect yourself from RedEnergy:

- Be careful about what links you click on and what attachments you open.

Keep your software up to date.

Use a firewall and antivirus software.

Back up your data regularly.

If you think you have been infected with RedEnergy, you should:

Disconnect from the internet.

Do not pay the ransom.

Contact a cybersecurity professional for help.

Additional Details About RedEnergy

The malware is written in .NET and is obfuscated to make it more difficult to analyze.

It uses HTTPS to communicate with its command and control servers, which makes it more difficult to block.

It has a number of different modules that allow it to steal a wide variety of data, including:

Web browser history

Email addresses and passwords

Credit card numbers

Crypto wallet keys

The ransom note that is displayed to victims is typically written in English, but it can also be translated into other languages.

The attackers behind RedEnergy are still active and have been observed targeting new victims in recent weeks.

Tips for Protecting Yourself from RedEnergy

Be suspicious of any emails or attachments that you receive from unknown senders.

Do not click on links in emails unless you are sure they are legitimate.

Keep your operating system and software up to date with the latest security patches.

Use a firewall and antivirus software to protect your computer from malware.

- Back up your data regularly so that you can restore it if it is encrypted by ransomware.

Conclusion

RedEnergy is a serious threat that should be taken seriously. By following the tips above, you can help protect yourself from this threat.

I hope this article helps you stay safe from RedEnergy and other ransomware threats.
Sources:

RedEnergy Stealer-as-a-Ransomware Threat Targeting Energy and Telecom Sectors
Extra Tags:

- RedEnergy
- stealer-as-a-ransomware (StAR) threat
- fake browser update campaigns
- web browsers
- email clients
- password managers
- crypto wallets
- file-sharing services