P

Petya Ransomware: How it locks Windows systems and how to respond

What it is Petya is a ransomware family first seen in 2016 that targets Windows boot and file-system structures rather than encrypting ordinary documents one by one. Original variants replaced the master boot record and encrypted the...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
1 min

What it is

Petya is a ransomware family first seen in 2016 that targets Windows boot and file-system structures rather than encrypting ordinary documents one by one. Original variants replaced the master boot record and encrypted the NTFS master file table, preventing Windows from locating files and starting normally.

How it works

Early campaigns used phishing messages and malicious files. After gaining the required privileges, Petya restarted the computer and displayed a fake disk-check screen while damaging access to the file system, followed by a ransom demand. Some campaigns paired Petya with

another component that encrypted files when administrative access was unavailable.

Key points

- Petya and NotPetya share visual and technical elements, but NotPetya was a destructive 2017 attack with no reliable payment-based recovery.
- A locked boot screen does not prove files are securely recoverable through the attacker.
- Disk images and variant identification should be preserved before attempting repair tools.

What to do

- Disconnect the device and avoid repeated boots or unverified repair commands.
- Create a forensic copy or work with a recovery specialist when data is important.
- Remove the infection or rebuild the system before restoring clean backups.
- Use email controls, least privilege, patching, and offline backups to reduce future impact.