P

Petya Ransomware: The 2016 Malware and Safe Recovery

Original Petya ransomware appeared in 2016 and prevented Windows from accessing files by targeting boot and NTFS structures. It is distinct from the 2017 NotPetya wiper.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 How original Petya worked

02 Petya vs. Mischa, GoldenEye, and NotPetya

03 Signs of a Petya-style incident

04 Immediate response

05 Decryption and recovery options

06 Safe recovery workflow

07 Prevention

08 Frequently asked questions

Quick answer: Petya is a Windows ransomware family first observed in 2016. Instead of encrypting ordinary documents one by one, original Petya variants replaced boot code and encrypted the NTFS Master File Table (MFT), preventing the operating system from

locating files. Petya is not the same incident as NotPetya, the destructive 2017 malware that borrowed Petya's appearance.

01 How original Petya worked

Historic Petya campaigns used social engineering, including files presented as job applications. When a victim launched the executable and granted administrative privileges, the malware modified the Master Boot Record (MBR) and arranged to run its own code after a restart. It displayed a fake disk-check screen while transforming the MFT, then showed a ransom demand.

The MFT is the index Windows uses to map filenames and metadata to data on an NTFS volume. Encrypting that index makes the volume appear inaccessible even though the attack does not necessarily encrypt every file's contents individually. Modifying boot structures also prevents a normal Windows startup.

02 Petya vs. Mischa, GoldenEye, and NotPetya

- **Petya:** the original family targeting boot and NTFS structures.
- **Mischa:** a related payload reported in campaigns where Petya could not obtain the privileges needed for its disk-level behavior; it encrypted files instead.
- **GoldenEye:** a later combined campaign or variant name associated with both file and disk encryption behavior.
- **NotPetya:** the June 2017 destructive outbreak that reused Petya-like code and a ransom screen but had different delivery, propagation, and recovery properties.

The distinction affects recovery. Early Petya implementations contained weaknesses that researchers could use in some cases. NotPetya did not provide a practical attacker-controlled recovery path and should be treated as a wiper. See the separate NotPetya recovery lessons for the 2017 event.

03 Signs of a Petya-style incident

- A Windows device restarts unexpectedly after a suspicious executable is opened.
- A disk-check screen appears outside expected maintenance, followed by a ransom screen.
- The system can no longer boot normally or the NTFS volume appears inaccessible.
- Email or download records show a disguised executable shortly before the restart.
- Security tooling identifies Petya, Mischa, GoldenEye, or a related sample.

These symptoms are not unique. Disk failure, boot corruption, and other malware can look similar. Preserve the drive image, ransom-screen details, original suspicious file, relevant email, and security telemetry. Confirm the exact family and variant before attempting a repair or decryptor.

04 Immediate response

1. **Isolate the affected device.** Disconnect networks and removable storage to protect shares and preserve evidence.
2. **Do not repeatedly reboot it.** Additional boot attempts and unverified repair tools may complicate recovery.
3. **Protect accounts.** If the initial file or a related payload may have stolen credentials, reset them from a clean device and revoke sessions.
4. **Determine scope.** Find the delivered file, recipients, execution events, and any related infections.
5. **Image the disk when data matters.** A qualified responder can work from a copy rather than the only damaged drive.

05 Decryption and recovery options

Recovery depends on the specific Petya generation. Security researchers documented flaws in certain 2016 variants, but a method for one version does not apply to all Petya-like malware. Use a reputable ransomware identification service and the No More Ransom repository to find vetted

tools. Test only on a copy or cloned disk.

For business systems or irreplaceable data, avoid general-purpose boot repair and random utilities before forensic imaging. Rebuilding the operating system and restoring clean data is often safer than trusting a repaired host whose original compromise is not understood. Paying offers no guaranteed result and may create legal or sanctions issues.

06 Safe recovery workflow

1. Identify the sample and separate original Petya from NotPetya and unrelated imitators.
2. Find and block the delivery path, including the email, download source, or compromised account.
3. Preserve or clone affected storage and test any supported recovery method on the copy.
4. Reinstall Windows from trusted media when system integrity cannot be established.
5. Restore documents from an offline backup made before infection; do not restore unknown executables.
6. Patch, enable endpoint protection, and monitor accounts and systems after reconnection.

07 Prevention

Block disguised executables and dangerous archive contents at email and web gateways. Show full file extensions, prevent standard users from gaining administrator rights casually, and use application control for downloaded code. Keep Windows and security tools supported and updated. Segment file shares and limit write permissions.

Maintain offline or immutable backups and test bare-metal and file restoration. A disk-focused attack can make the whole system unbootable, so recovery plans need installation media, configuration records, and identity access—not just copies of individual documents.

08 Frequently asked questions

Are Petya and NotPetya the same malware?

No. They share code and visual traits, but the 2017 NotPetya attack had different propagation and destructive recovery characteristics.

Does the fake disk check encrypt files?

Original Petya used that stage while encrypting the NTFS file table, which prevented Windows from locating files on the volume.

Should I run Windows boot repair first?

Not when important data or evidence is at stake. Isolate and image the drive, identify the variant, and use a vetted recovery plan.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com