N

NotPetya: The 2017 Destructive Wiper and Recovery Lessons

NotPetya was a destructive 2017 cyberattack disguised as ransomware. Learn how it entered and spread, why payment could not restore data, and what it taught defenders.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 NotPetya, Petya, and ordinary ransomware
02 How the 2017 attack began
03 How NotPetya spread inside networks
04 What the malware damaged
05 What to do in a destructive outbreak
06 Defensive lessons that still matter
07 Frequently asked questions

Quick answer: NotPetya was a destructive malware attack that began on June 27, 2017 and presented victims with a ransom demand. Unlike ordinary ransomware designed to provide a unique decryption path after payment, NotPetya's implementation made reliable recovery through the attacker impossible. It is therefore best understood as a wiper disguised as ransomware.

01 NotPetya, Petya, and ordinary ransomware

NotPetya borrowed code and visual characteristics from earlier Petya ransomware, which is why early reports used names such as Petya, ExPetr, or GoldenEye. The attacks should not be treated as identical. Microsoft's overview of the Petya/NotPetya attack explains that the ransom screen did not correspond to a technical process for generating and registering individual recovery keys.

Normal ransomware is financially motivated and usually attempts to preserve the possibility of decryption because that possibility supports payment. NotPetya caused irreversible disruption at scale. Calling it only "ransomware" hides the central operational lesson: organizations needed clean reconstruction and business-continuity procedures, not a payment path.

02 How the 2017 attack began

Investigations tied the initial wave to a compromised software update mechanism for M.E.Doc, accounting software widely used in Ukraine. A trusted business application therefore became the delivery channel into customer environments. The event is a landmark example of software supply-chain risk: a victim could receive the malicious code through an expected update rather than a suspicious attachment.

The exact 2017 distribution history is important context, not a current indicator that every M.E.Doc installation or every destructive outbreak is NotPetya. Current incidents require current evidence.

03 How NotPetya spread inside networks

Once running, NotPetya combined several propagation methods:

- credential dumping from memory to obtain usable accounts;
- administrative execution with tools and mechanisms such as PsExec and WMIC;
- discovery of other workstations, servers, and network ranges;
- SMB exploitation associated with MS17-010, including EternalBlue and EternalRomance, where systems were vulnerable.

Microsoft's technical analysis of NotPetya propagation documents credential use, administrative shares, remote execution, and optional SMB exploitation. This combination explains why patching MS17-010 was necessary but not sufficient: stolen administrative credentials could still enable movement to fully patched hosts.

04 What the malware damaged

NotPetya modified disk structures and forced a restart before showing a ransom screen. On affected systems, the result could prevent Windows from starting and make data inaccessible. Because the attack also moved rapidly through enterprise networks, shared dependencies, authentication systems, and operational technology interfaces could amplify business impact far beyond one workstation.

An old "vaccine" technique based on creating a local filename was widely discussed during the outbreak, but it was not a complete security control and did not remediate an intrusion. Durable lessons are segmentation, credential protection, patching, controlled software updates, detection, and recoverable backups.

05 What to do in a destructive outbreak

1. **Activate incident and continuity plans.** Treat widespread boot failure or rapid destructive changes as an enterprise emergency.
2. **Isolate affected network segments.** Restrict SMB and administrative movement while preserving essential safety functions.
3. **Protect identities.** Assume credentials used on compromised endpoints may be exposed; restrict privileged accounts and rotate secrets from clean systems in a controlled order.

4. **Preserve evidence.** Retain representative disks, memory where available, logs, update records, and network telemetry before rebuilding everything.
5. **Establish a clean recovery environment.** Verify identity, DNS, management, and security infrastructure before reconnecting restored business systems.
6. **Rebuild rather than trust damaged hosts.** Use known-good installation media and validated configurations, then restore clean data according to business priority.

Do not assume the ransom address or payment instructions provide recovery. In a suspected modern wiper event, contact qualified incident responders and relevant national cybersecurity or law-enforcement authorities.

06 Defensive lessons that still matter

Patch critical vulnerabilities, but also prevent credential-based lateral movement. Separate privileged accounts from daily use, use secured admin workstations, restrict local administrator reuse, and monitor remote service creation and administrative shares. Segment networks so compromise of one business application cannot freely reach every endpoint.

Evaluate the security of software-update channels and third-party access. Inventory dependencies, validate signatures and update sources, centralize endpoint and identity telemetry, and plan how to suspend a supplier connection safely. Maintain offline or immutable backups with different credentials and perform realistic restoration exercises that include loss of domain services and management tools.

07 Frequently asked questions

Was NotPetya ransomware?

It displayed a ransom demand and reused ransomware-like code, but its destructive design did not provide a reliable attacker-controlled recovery mechanism. Wiper is the more accurate operational classification.

Did EternalBlue cause every infection?

No. NotPetya also used stolen credentials and legitimate administrative execution methods. Patched systems could still be reached with valid privileged credentials.

Can NotPetya still run today?

Historic samples remain dangerous in poorly protected environments, but modern destructive incidents should not be attributed to NotPetya without technical evidence.

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