N

NotPetya: Why this destructive attack was not ordinary ransomware

What it is NotPetya is destructive malware used in a global attack in June 2017. It displayed a ransom demand and reused ideas from Petya, but its design made reliable recovery through payment impossible. For that reason, NotPetya is...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
1 min

What it is

NotPetya is destructive malware used in a global attack in June 2017. It displayed a ransom demand and reused ideas from Petya, but its design made reliable recovery through payment impossible. For that reason, NotPetya is widely treated as a wiper masquerading as ransomware rather than a normal profit-driven ransomware campaign.

How it works

The initial compromise was distributed through a poisoned update mechanism for Ukrainian accounting software. Inside networks, the malware spread rapidly using credential theft and Windows administrative techniques, as well as an SMB exploit on vulnerable systems. It damaged

boot and file-system structures, preventing normal access to data and disrupting organizations far beyond the original targets.

Key points

- NotPetya and the earlier Petya ransomware family are related in appearance but should not be treated as identical incidents.
- Patching one exploit was important, but stolen administrator credentials also enabled movement between patched systems.
- Connected business partners and trusted software channels can become high-impact supply-chain paths.

What to do

- Isolate affected networks and protect clean identity and backup infrastructure.
- Rebuild systems from trusted media rather than relying on ransom instructions.
- Rotate privileged credentials and review software deployment and update trust.
- Segment networks and restrict administrative protocols to reduce rapid lateral movement.