

# Cyber-espionage group GreyEnergy related to TeleBots exposed | ESET

Archived: 2026-04-05 13:29:08 UTC

## GreyEnergy finally exposed

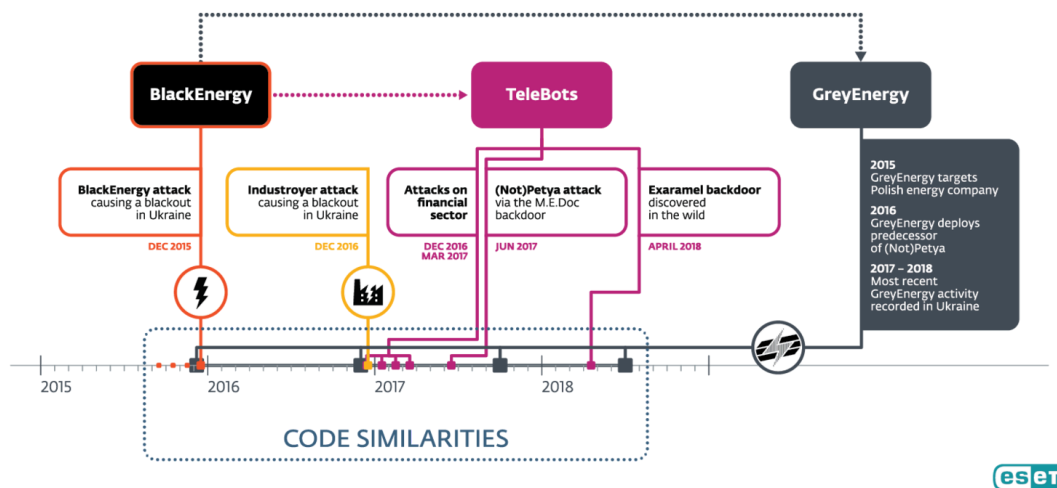
ESET researchers just [unmasked the shadowy cyber-espionage group](#) dubbed GreyEnergy. It's the successor to the BlackEnergy APT group which went 'underground' a few years ago after terrorizing Ukraine until 2015. It's also closely related to TeleBots, responsible for NotPetya, perhaps the most damaging cyberattack experienced.

Our researchers have demonstrated beyond doubt that GreyEnergy's malware toolkit both **mirrors and improves on already-sophisticated techniques** used in the devastating NotPetya attacks and Ukraine power grid outages.

ESET's exposure of GreyEnergy is important for a successful defense against this particular threat actor as well as for better understanding the tactics, tools and procedures of the most advanced APT groups.

Anton Cherepanov, ESET Senior Malware Researcher

## Links between BlackEnergy, Industroyer and GreyEnergy



## Organizations at risk

The consequences for organizations of all sizes can be devastating. Compared to BlackEnergy, GreyEnergy is a more modern toolkit with an even **greater focus on stealth**. ESET researchers have demonstrated that GreyEnergy has the capacity to **take full control of entire company networks**.

One basic stealth technique is to push only selected modules to selected targets, and only when needed. In addition, some GreyEnergy modules are partially encrypted and some remain fileless – running only in memory –

with the intention of hindering analysis and detection.

To cover their tracks, typically, GreyEnergy's operators securely wipe the malware components from the victims' hard drives.

The modules described in ESET's analysis were used for **espionage and reconnaissance** purposes and include: backdoor, file extraction, taking screenshots, keylogging, password and credential stealing.

### **How ESET protects you**

The good news is ESET can fully protect your organization. Our multilayered technology combining machine learning, human expertise and global threat intelligence, **combats exactly this type of new, previously unseen threat.**

Stay safe with ESET

### **ESET fully protects your organization from GreyEnergy**

---

Source: <https://www.eset.com/int/greyenergy-exposed/>