

# Advanced Persistent Threats

An advanced persistent threat (APT) is a well-resourced intruder that breaks into a network and stays hidden for months or years. Here is what it means for your organisation, and the mindset that keeps one out.

## WHAT IT IS

An APT is a prolonged, targeted intrusion, usually run by or for a nation-state. The aim is not a quick payout but long-term access, used to steal data, prepare sabotage or move into connected systems. You do not have to be the direct target to be hit. Many organisations are caught as collateral damage or used as a route into a bigger one.

## WHY IT MATTERS

### At least 5 years

That the Volt Typhoon group stayed hidden in some critical-infrastructure networks.

CISA, NSA and FBI, 2024

### Over 10 billion dollars

In worldwide damage from the NotPetya attack in 2017, much of it collateral.

US Department of Justice, 2020

### 38 percent

Of analysed EU cyber incidents hit public institutions, the most-targeted sector.

ENISA Threat Landscape, 2025

## WHAT HAPPENED

In December 2020 attackers hid a backdoor in a routine SolarWinds software update. About 18,000 organisations installed it, and the intruders quietly reached US government departments before anyone noticed. In April 2021 the US and UK attributed the campaign to Russia's foreign intelligence service, tracked as APT29. (NSA, CISA and FBI, 2021)

## RED FLAGS TO WATCH FOR

**APTs are built to blend in, so watch for unusual patterns rather than obvious malware.**

- Logins at odd hours or from unusual places, especially for admin accounts.
- Dormant or service accounts that suddenly become active.
- Unusual internal traffic as an intruder moves between machines.
- Data being gathered or sent to unfamiliar destinations.

## THE ONE RULE THAT STOPS IT

**Monitor continuously and assume an attacker could already be inside, because APTs are caught by spotting unusual behaviour long before any alarm sounds.**

## THEN BUILD THE HABIT AROUND IT

- Enforce phishing-resistant multi-factor authentication and least privilege.

- Segment the network so one foothold cannot reach everything.
- Patch internet-facing systems quickly, as they are common entry points.
- Keep offline, tested backups and a rehearsed incident response plan.

## MYTHS AND FACTS

### MYTH

We are too small to be an APT target.

### FACT

Size is not the filter. A small supplier to a large organisation can be the way in, and many victims are simply collateral damage.

### MYTH

Antivirus will catch an APT.

### FACT

Many APTs use legitimate built-in tools, so there is no malware signature. Behavioural monitoring is what finds them.

### MYTH

If we were breached, we would know.

### FACT

APTs are built to stay hidden. Some have gone undetected for years, like Volt Typhoon in US infrastructure.

## THE LEGAL DUTY

Continuous monitoring, supply-chain security and fast incident reporting are now legal duties under NIS2, in force in Sweden as Cybersäkerhetslagen since 15 January 2026, with boards personally accountable under Article 20.

---

## GET HELP

**eBuilder Security** provides managed detection and response that helps organisations spot advanced threats early. Read the full guide at the link below.

[Read the Full Article →](#)