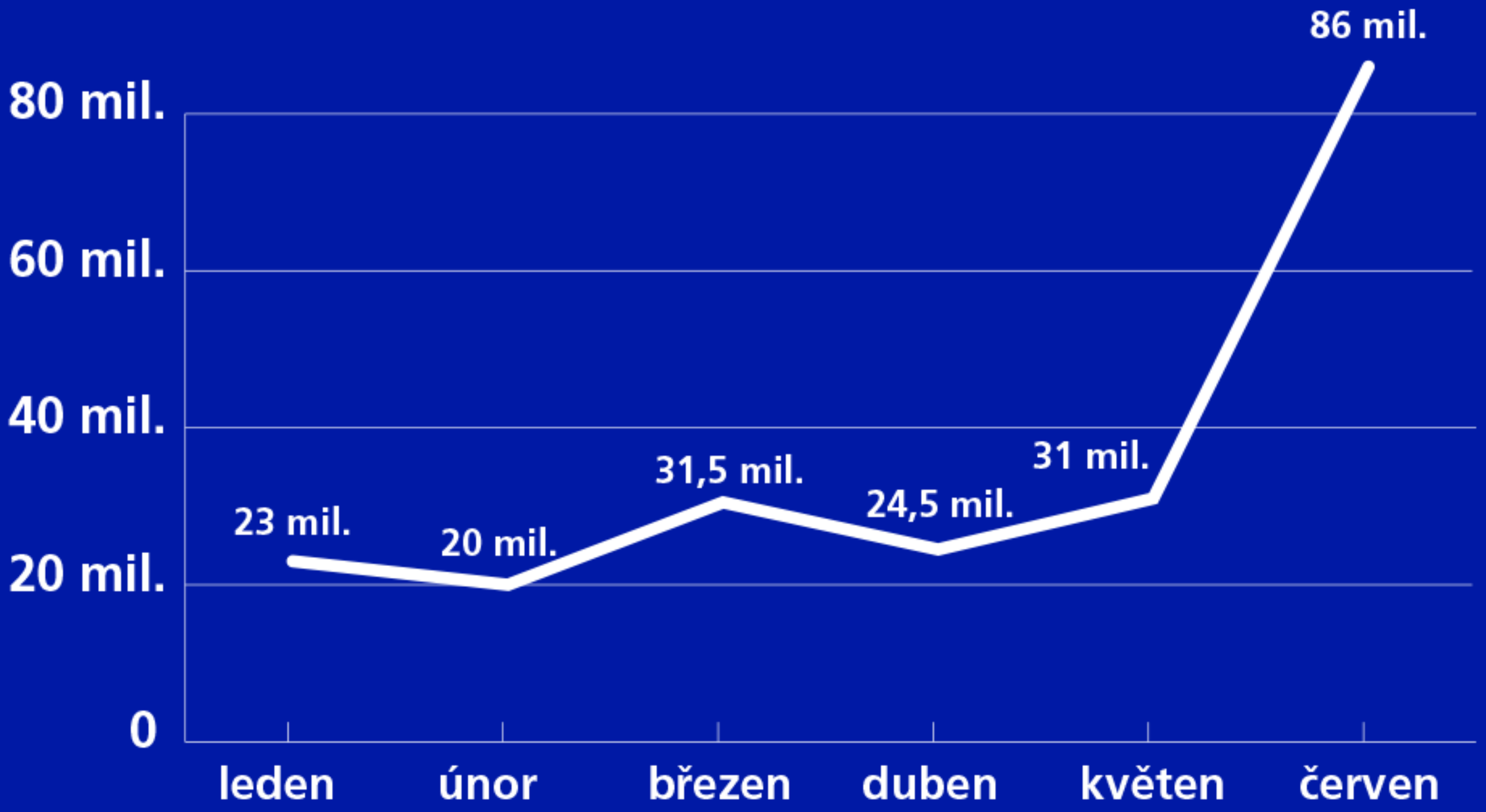
O2 CyberNews

V prvním pololetí roku 2023 jsme zabránili

216 000 000

hrozbám díky službě O2 Security.

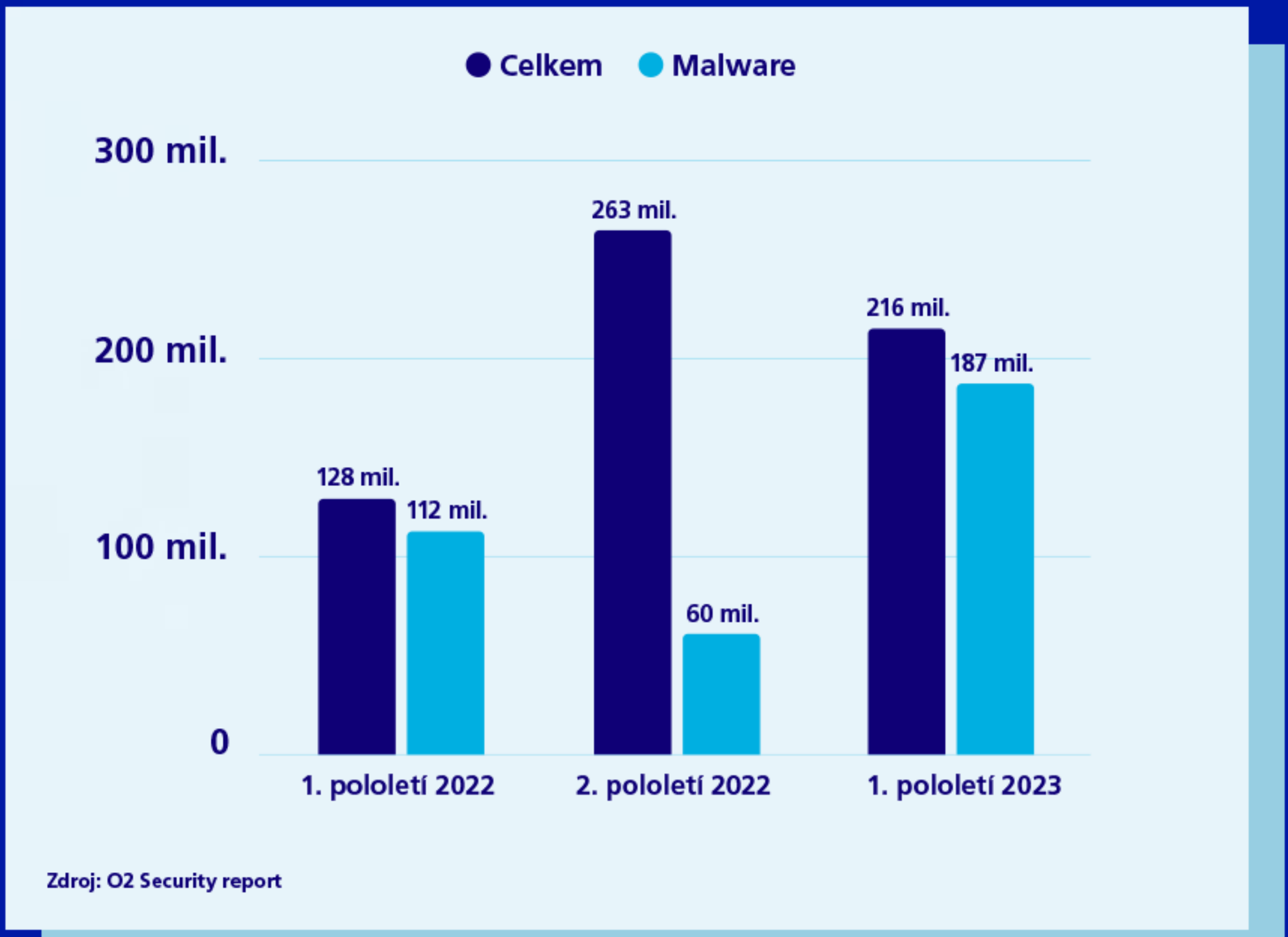
Počet kyberútoků v červnu vzrostl na 86 milionů



Hackeři byli nejaktivnější v červnu, kdy došlo k nejvíce pokusům o kyberútok od září minulého roku.

Zdroj: O2 Security report

Počty kybernetických hrozeb za poslední tři pololetí



Zdroj: O2 Security report

Nejčastější hrozby za první půlrok 2023

Phishing

–

Malware

–

Command & Control

Phishing

se ocitl v Top 3 hrozbách. PROČ? Jedním z možných důvodů může být adopce používání AI, která je schopna psát přesvědčivé texty bez gramatických chyb. Tímto typem útoku hackeři stále častěji cílí na firmy.

Jaké byly nejčastější phishing útoky?

1. Falešný videohovor (často přes platformy jako Zoom, Microsoft Teams nebo Google Meet)

2. Falešné pracovní dokumenty (často v PDF nebo v Excelu)

3. Scareware (podvod, který oběti vyděsí zprávou o napadení jejich zařízení a nabídne jim „pomoc“)

Malware

Oproti druhému pololetí loňského roku narostl letos počet malware útoků trojnásobně.

Jaké jsou typy malware útoků?

1. **Počítačové viry**
šířící se kopírováním do jiných programů

2. **Ransomware**
malware šifrující data a požadující výkupné za jejich obnovení

3. **Trojské koně**
malware vydávající se za legitimní software s cílem získat neoprávněný přístup

Command & Control

C&C je kybernetický útok, při kterém útočník ovládá zařízení přes C2 server. Na dálku provádí útoky, krádeže dat či šíření škodlivého kódu. Tyto útoky jsou často neodhalitelné.

O2 CyberNews

Chcete se dozvědět více?

Podrobný O2 Security report najdete na:

www.o2cybernews.cz