ALEF

Zranitelný internet

aneb narůstající technologický dluh a s ním spojené hrozby

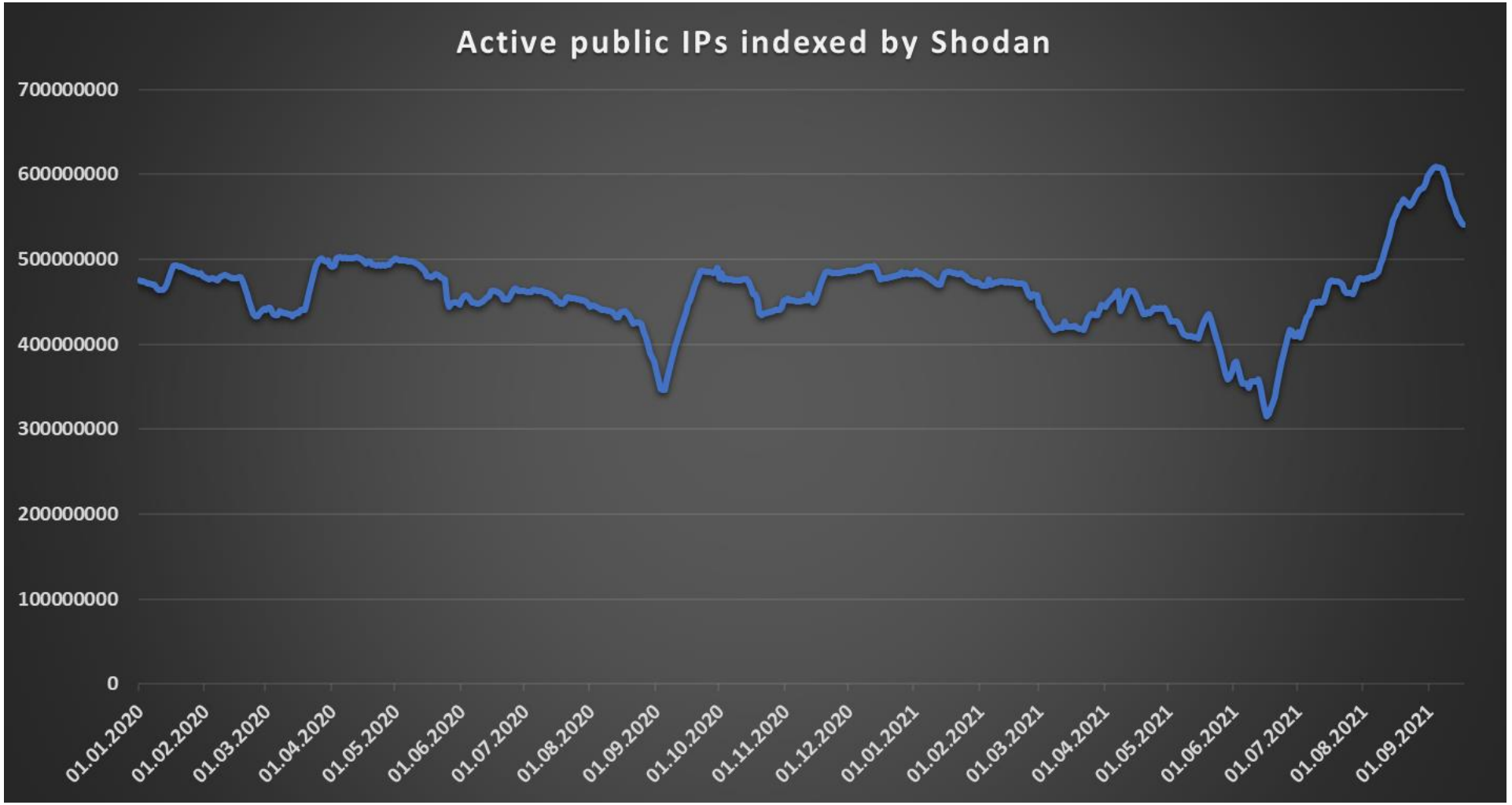
Jan Kopřiva

jan.kopriva@alef.com @jk0pr

ALEF CSIRT

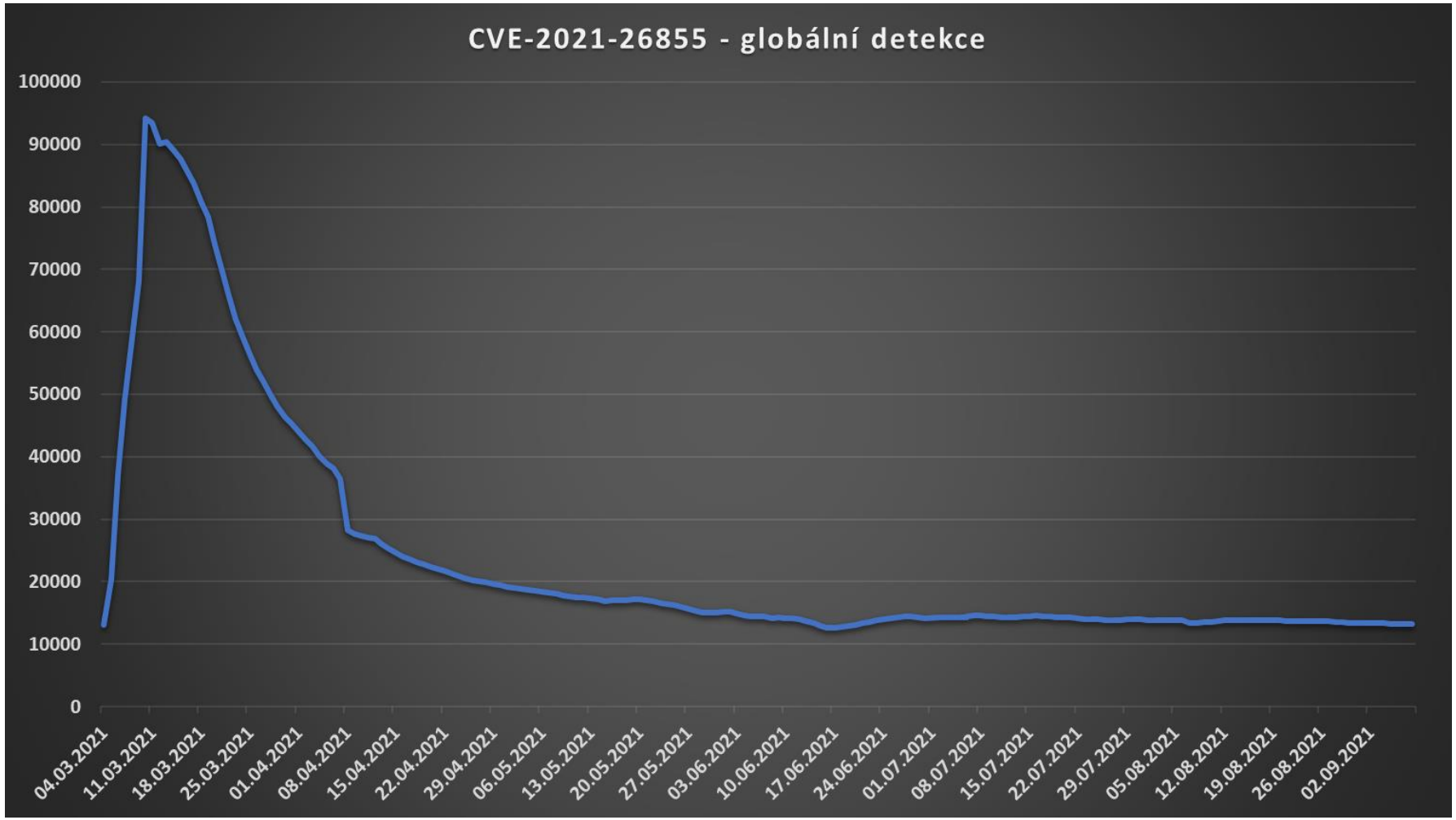
TLP: WHITE

Jak vypadá globální internet?



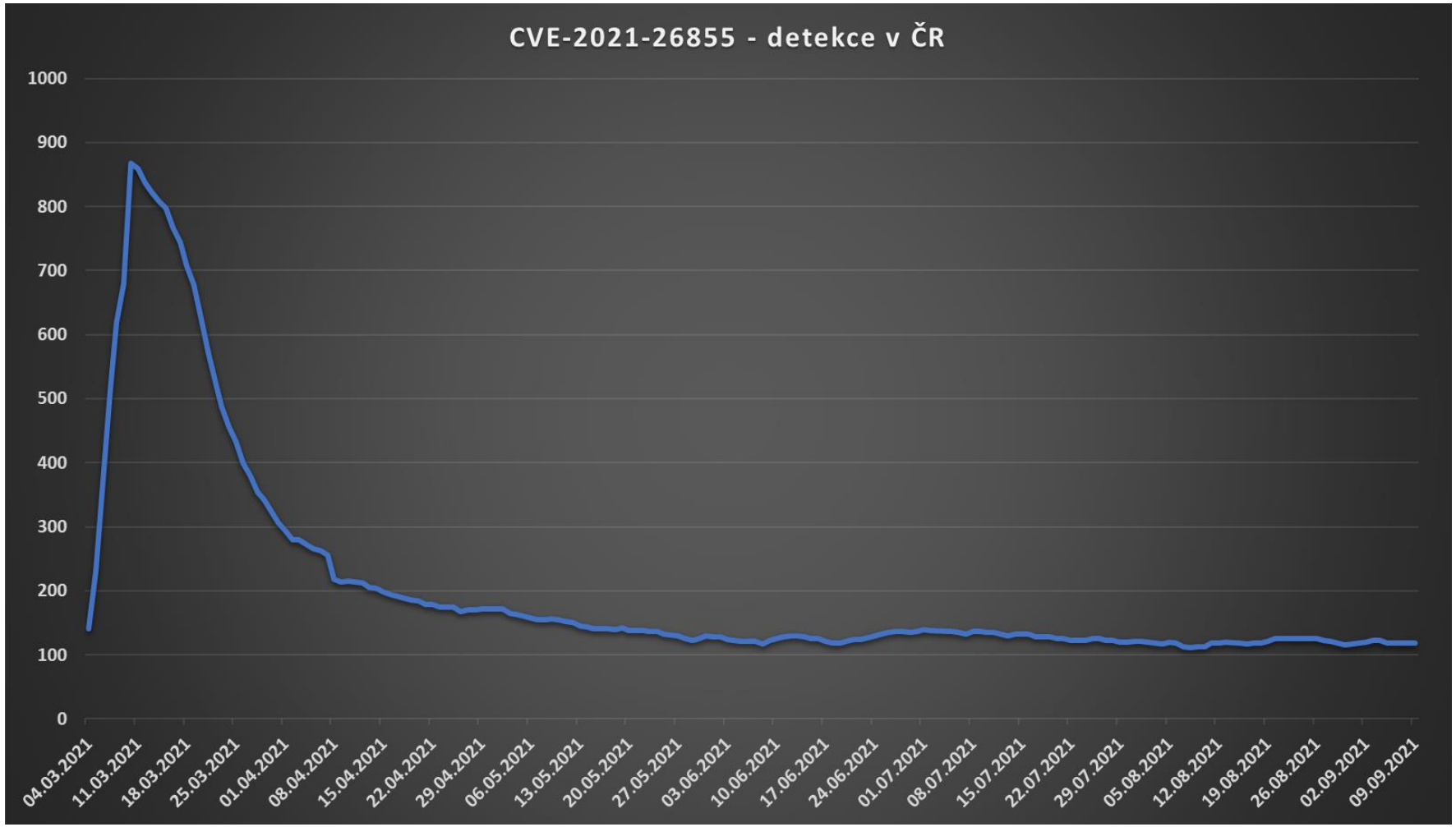
ALEF

Jak to vypadá s počty zranitelných systémů?



Zdroj: Shodan

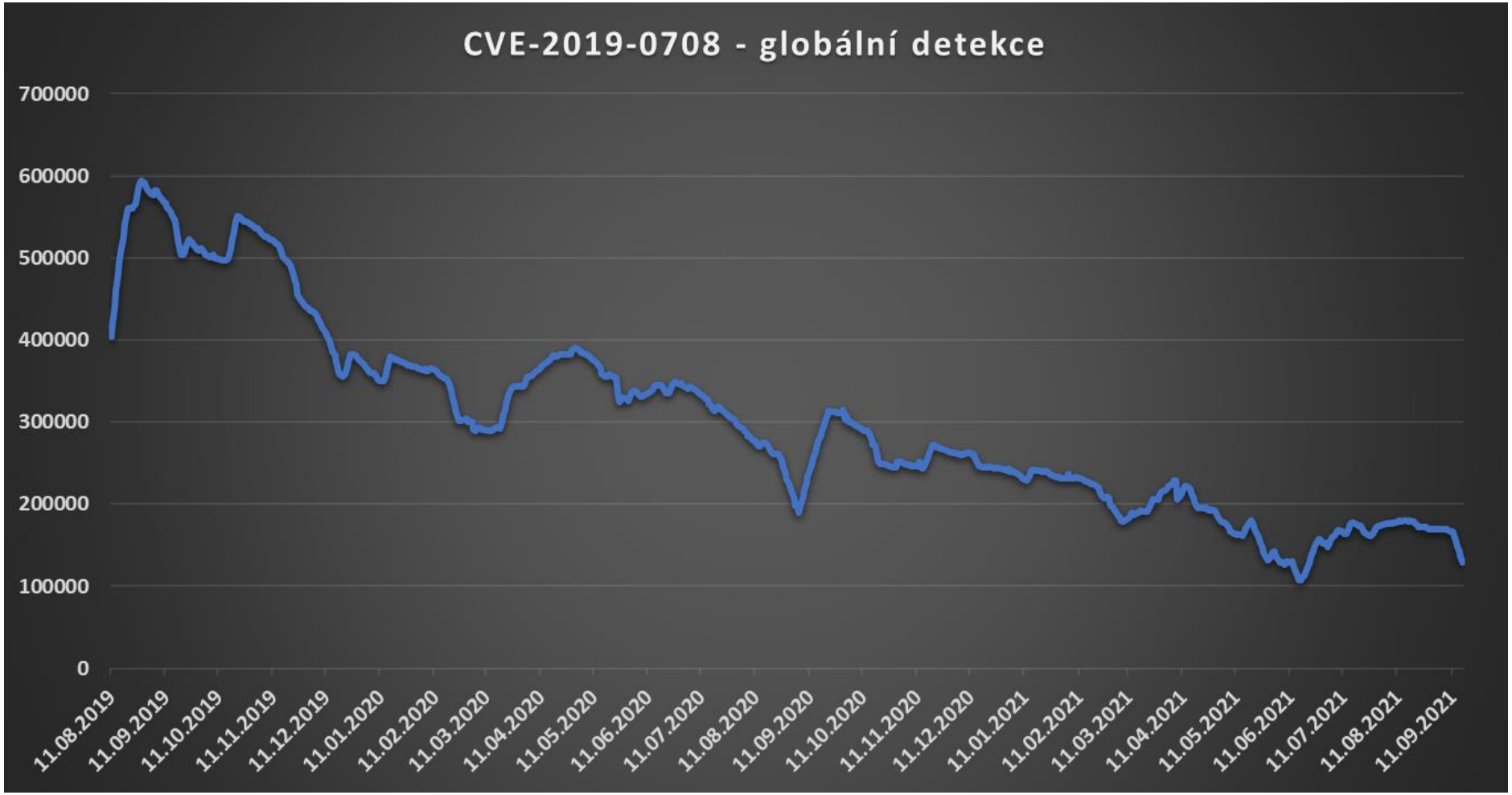
Jak to vypadá s počty zranitelných systémů?



ALEF

Zdroj: Shodan

Jak to vypadá s počty zranitelných systémů?



Source: Shodan

Zdá se, že všechno je v pořádku…

ALEF

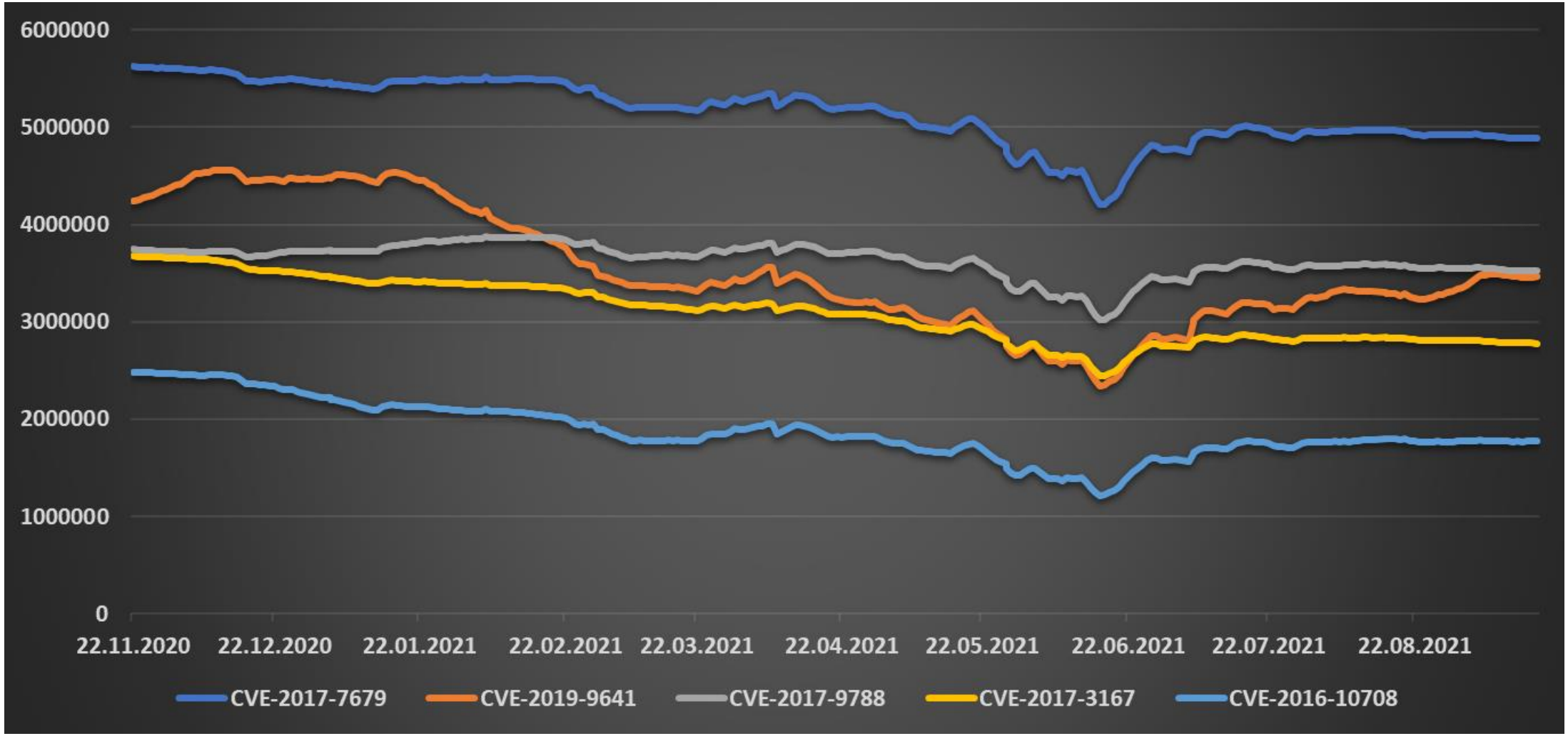
…ale je to opravdu tak?

ALEF

Co zranitelnosti, o kterých se nepíše/nemluví?

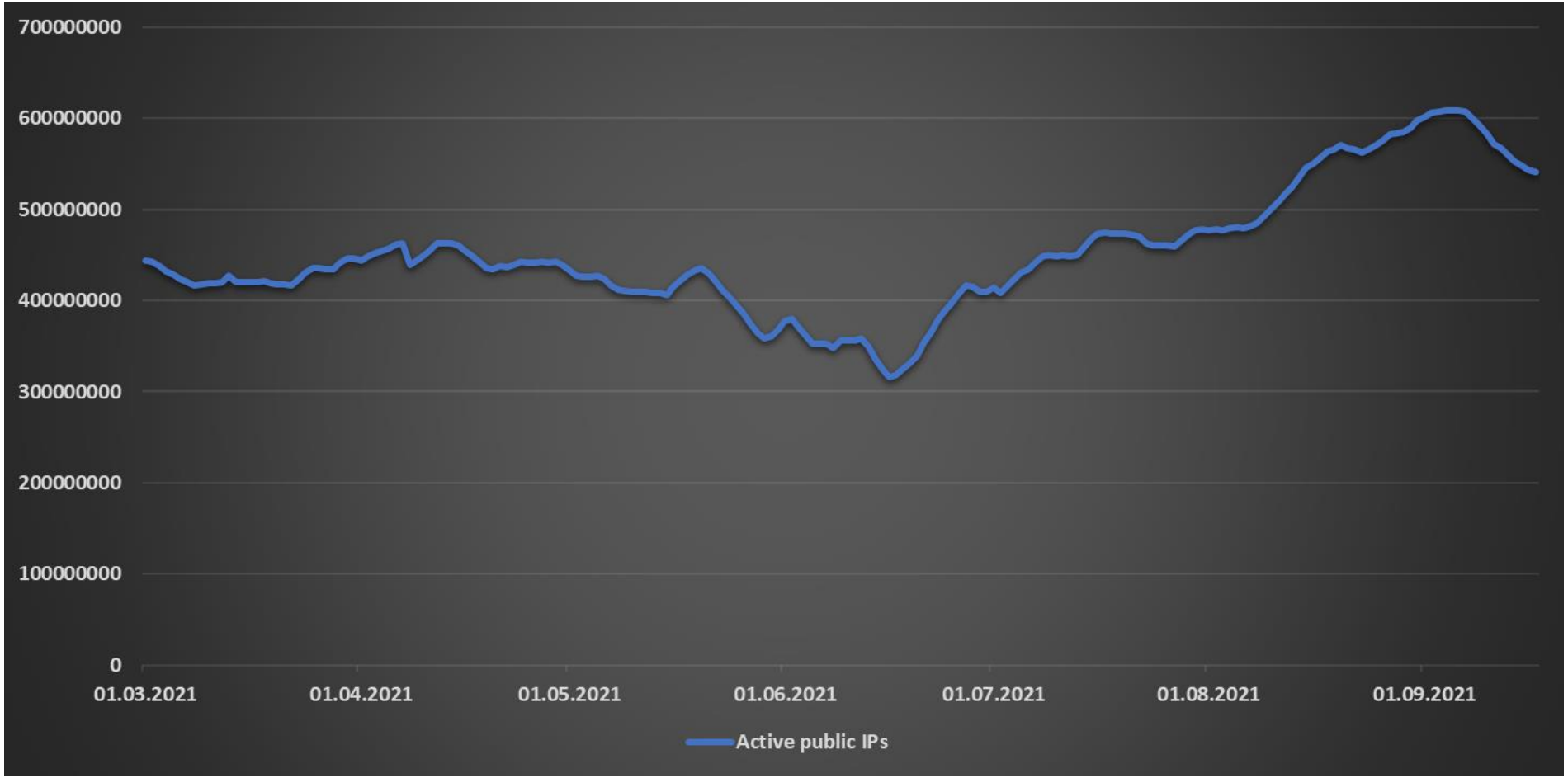
- CVE-2017-7679 - Buffer Over-read in Apache - CVSSv3: 9.8
- CVE-2019-9641 - Uninitalized read in PHP - CVSSv3: 9.8
- CVE-2017-9788 - Information leak in Apache - CVSSv3: 9.1
- CVE-2017-3167 - Authentication bypass in Apache - CVSSv3: 9.8
- CVE-2016-10708 - Null Pointer Dereference in OpenSSH - CVSSv3: 7.5

Co zranitelnosti, o kterých se nepíše/nemluví?



Source: Shodan

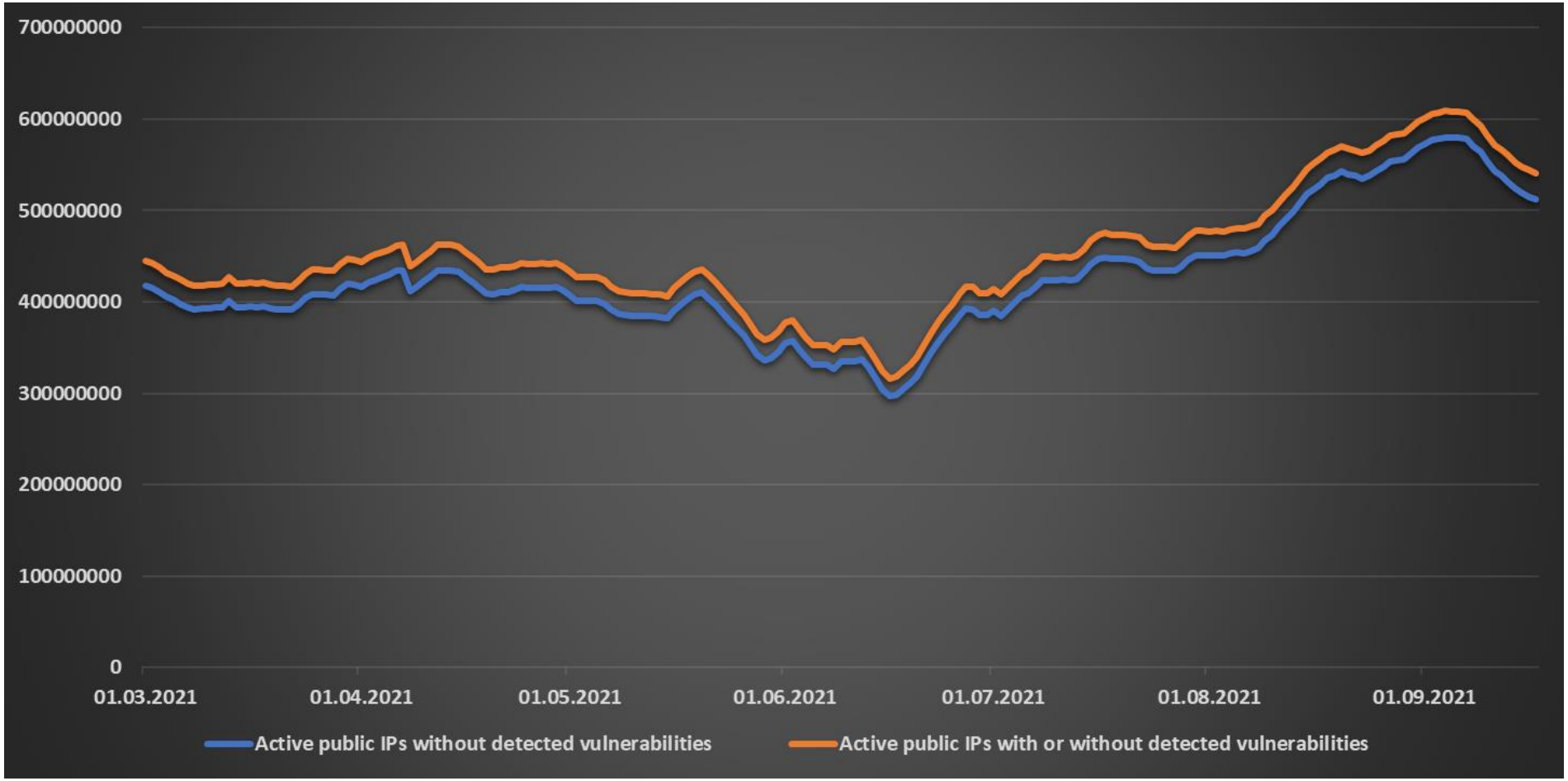
Co zranitelné systémy obecně?



ALEF

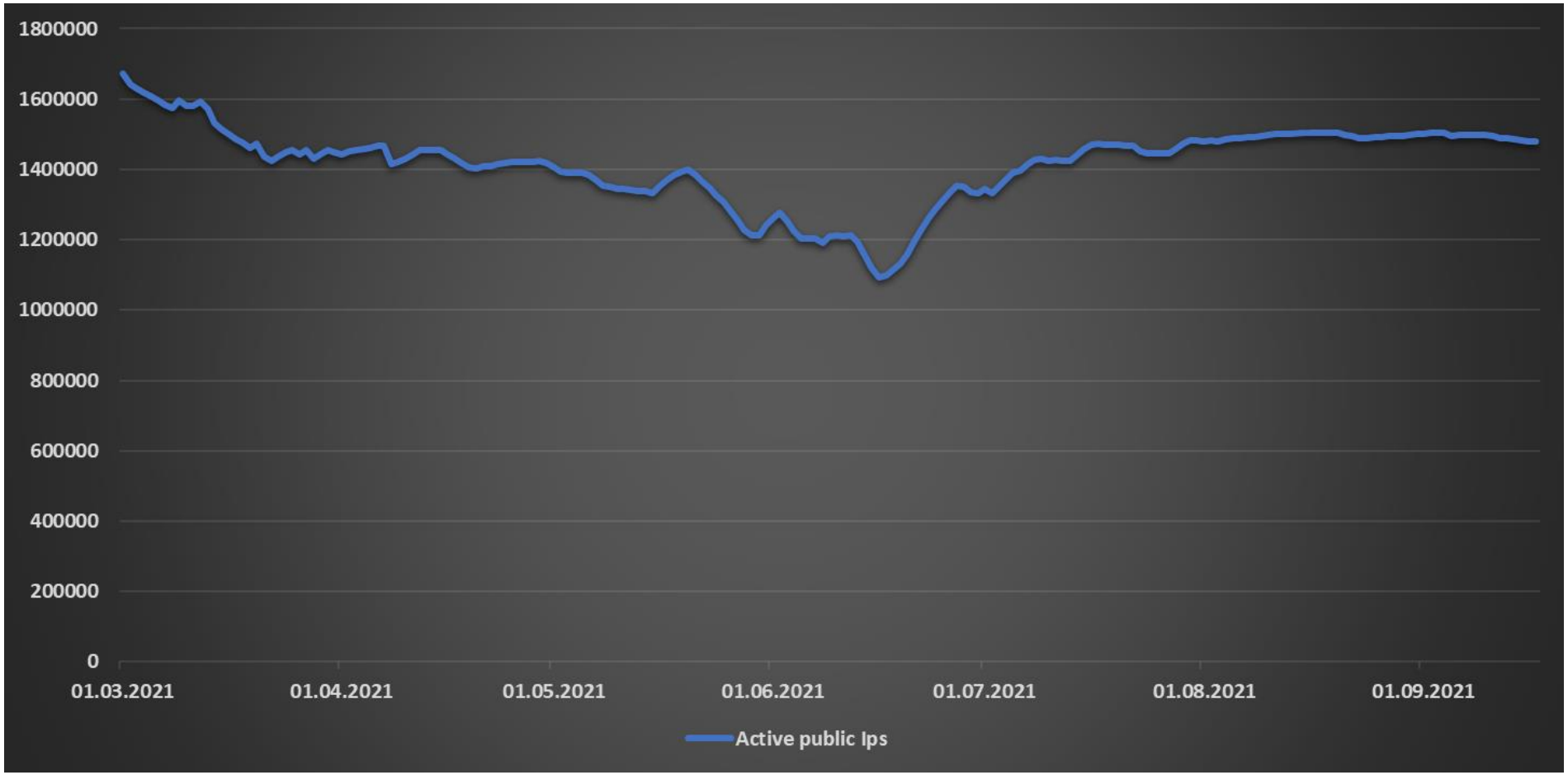
Source: Shodan

Co zranitelné systémy obecně?



Source: Shodan

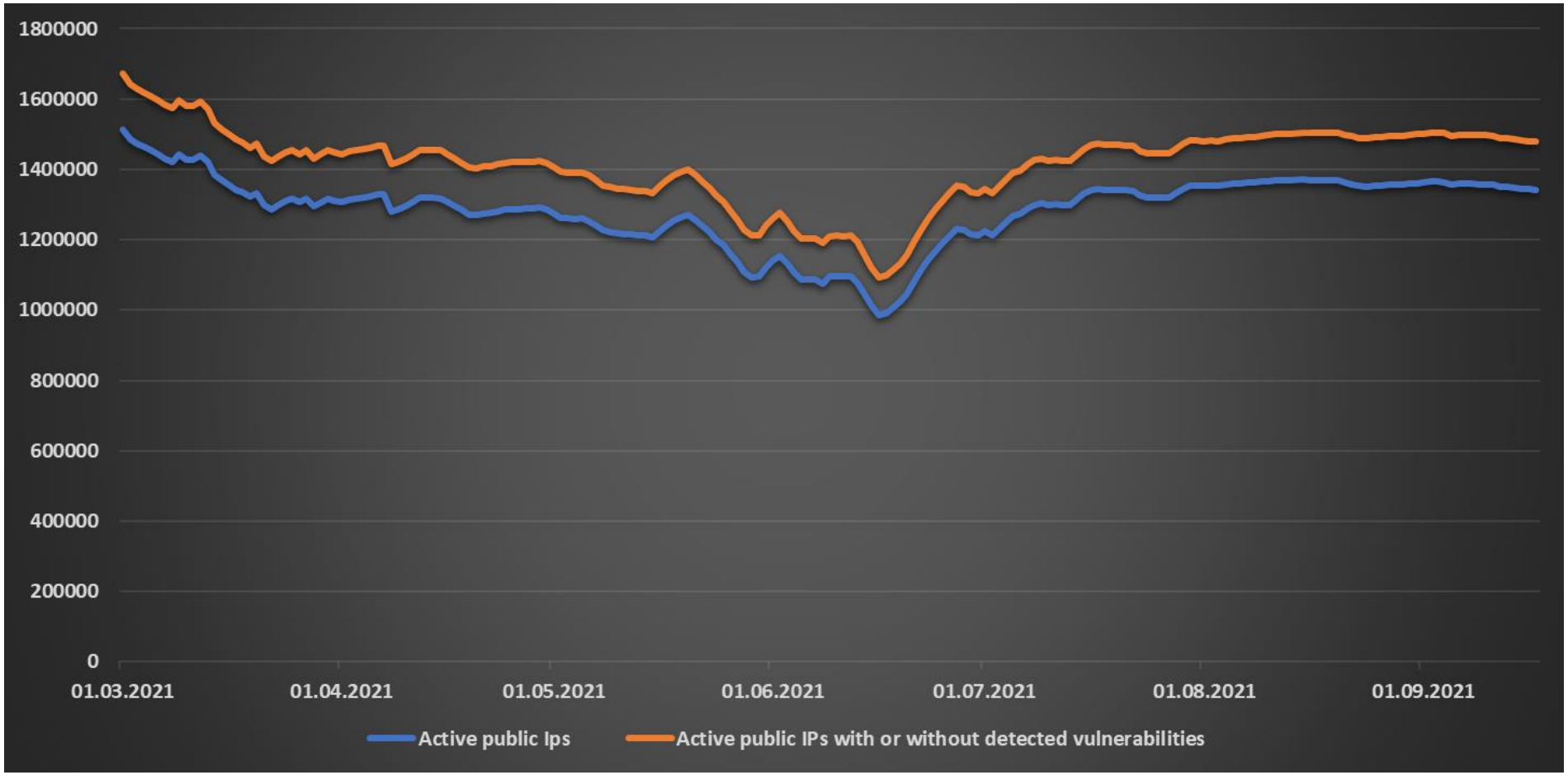
Situace v ČR



ALEF

Source: Shodan

Situace v ČR



ALEF

Source: Shodan

Zdá se, že všechno není zcela v pořádku…

ALEF

…ale je to problém pro nás?

- Máme-li záplatovanou a dobře chráněnou vlastní infrastrukturu, útoky na jednotlivá zranitelná zařízení se nás nedotknou
- Ale…
  - Masivní útoky na zranitelná zařízení mohou mít (extrémní) dopad na dostupnost
  - Útoky zneužívající zranitelná zařízení mohou cílit i na plně záplatovanou infrastrukturu

Aktuální situace

- Část zranitelných systémů je důsledkem "nedostatků" organizací v oblasti řízení bezpečnosti
- Ne všechna k internetu připojená zařízení mohou být aktualizována
  - EoS/EoL zařízení, IoT, nepovýšitelná SW báze…
- Stávající technologický dluh se bude v budoucnu kontinuálně navyšovat

Co přinese budoucnost?

- Současný přístup je nevyhovovující
- Nedávná praxe ukazuje zajímavé potenciální cesty
  - Distribuce „uninstall“ updatů pro nakažené stroje přes C2 infrastrukturu Emotet
  - Hack-to-clean Exchange serverů kompromitovaných s pomocí zranitelnosti ProxyLogon

Co přinese budoucnost?

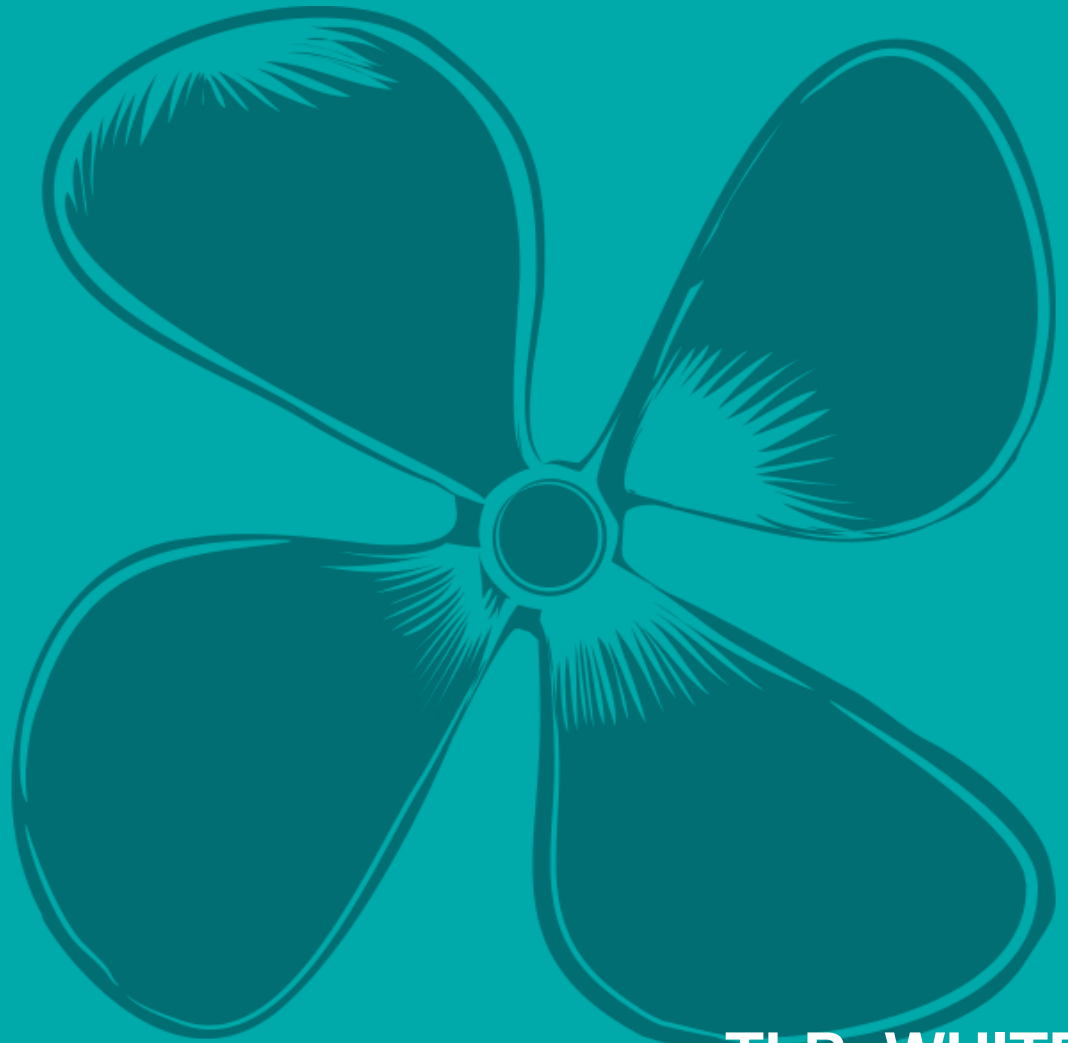
- Některé potenciální cesty mohou působit až drakonicky…
  - Zablokování připojení k internetu nakaženým strojům
  - Hack-to-clean
  - Hack-to-patch
- …jiné méně
  - Forced patching jako standard pro tvůrce HW/SW

Co přinese budoucnost?

- Bez ohledu na konečný způsob řešení musí nezbytně dojít ke změně paradigmatu…
- …doufejme jen, že dříve, než se začnou pravidelně objevovat botnety geograficky omezené na území jednoho státu, užívané k útokům na kritickou infrastrukturu státu jiného…
- …nebo se objeví další „Warholův červ“

ALEF

Děkuji Vám za pozornost!



TLP: WHITE