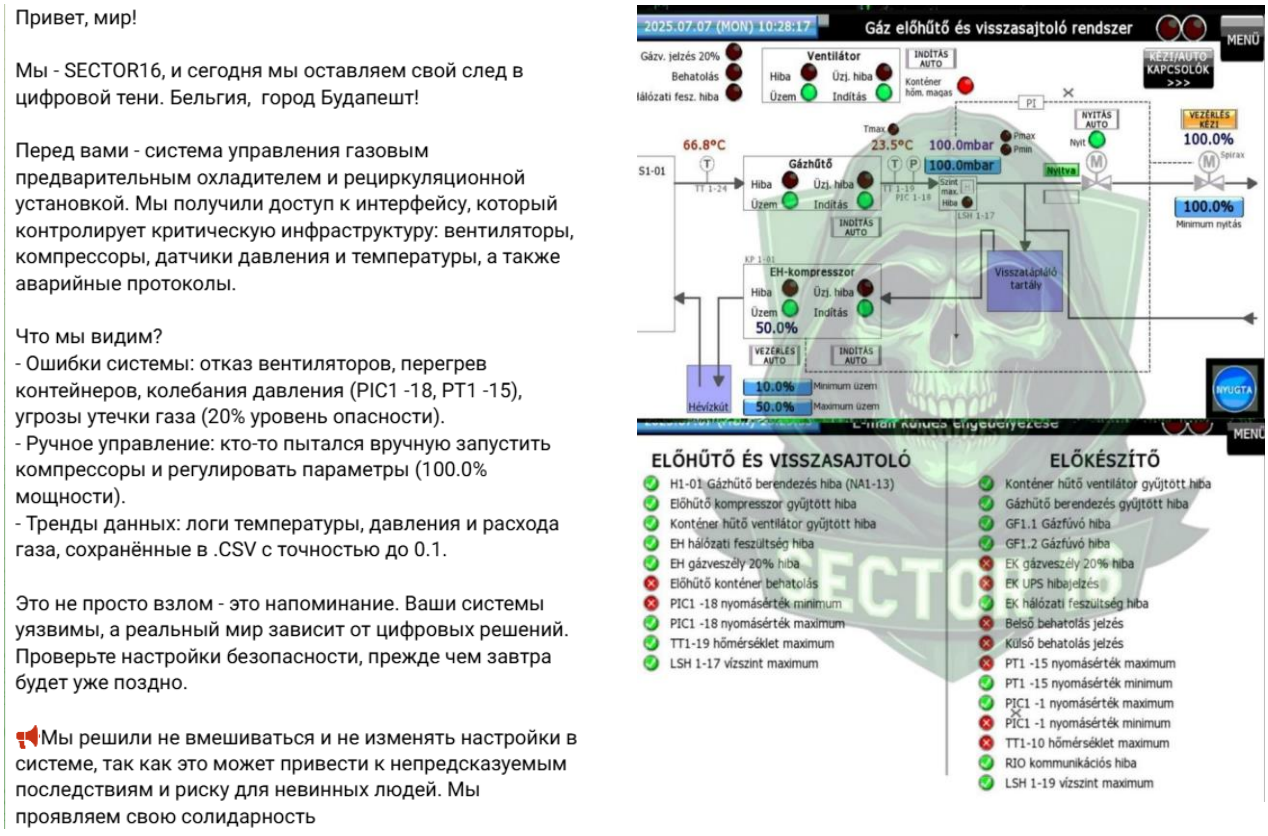
TLP:CLEAR
Szabadon terjeszthető!

Tájékoztatás
a SECTOR 16 csoport magyar geotermikus rendszer elleni támadásával kapcsolatban

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézete (NBSZ NKI) felhívja a figyelmet a SECTOR 16 nevű hackercsoport által elkövetett kibertámadásra, amely 2025 júliusában egy magyarországi geotermikus termelőrendszert célzott meg.

A támadók sikeresen behatoltak a termelőüzem kritikus vezérlési interfészébe, amely révén részletes betekintést nyertek a rendszer működésébe és biztonsági beállításaiba. Bár közvetlen beavatkozást, például beállítások módosítását vagy szabotázst nem hajtottak végre, figyelmeztető üzeneteket küldtek, amelyekben a rendszer sebezhetőségére, valamint a kiberbiztonsági hiányosságokra hívták fel a figyelmet.

A támadás során a rendszer működésében az alábbi zavarokat tárták fel: ventilátor leállás, túlmelegedés, illetve nyomásingadozás, amelyek potenciálisan veszélyeztethetik az üzembiztonságot. A támadók a behatolás bizonyítékait saját Telegram-csatornájukon is közzétették, ezzel demonstrálva a támadás sikerességét és nyomatékosítva figyelmeztető üzenetüket.



Привет, мир!

Мы - SECTOR16, и сегодня мы оставляем свой след в цифровой тени. Бельгия, город Будапешт!

Перед вами - система управления газовым предварительным охладителем и рециркуляционной установкой. Мы получили доступ к интерфейсу, который контролирует критическую инфраструктуру: вентиляторы, компрессоры, датчики давления и температуры, а также аварийные протоколы.

Что мы видим?
- Ошибки системы: отказ вентиляторов, перегрев контейнеров, колебания давления (PIC1 -18, PT1 -15), угрозы утечки газа (20% уровень опасности).
- Ручное управление: кто-то пытался вручную запустить компрессоры и регулировать параметры (100.0% мощности).
- Тренды данных: логи температуры, давления и расхода газа, сохранённые в .CSV с точностью до 0.1.

Это не просто взлом - это напоминание. Ваши системы уязвимы, а реальный мир зависит от цифровых решений. Проверьте настройки безопасности, прежде чем завтра будет уже поздно.

📢Мы решили не вмешиваться и не изменять настройки в системе, так как это может привести к непредсказуемым последствиям и риску для невинных людей. Мы проявляем свою солидарность

A hazai geotermikus termelőrendszerbe történt behatolás bizonyítékaként közzétett üzenet és kép.
Forrás: kiber.blog.hu

Az NBSZ NKI az eset kapcsán az alábbiakat javasolja:

- A kritikus infrastruktúrákat üzemeltető szervezetek rendszeresen végezzenek biztonsági felülvizsgálatokat az informatikai és ipari vezérlőrendszereken.
- Korszerűsítsék a védelmi intézkedéseket, különös tekintettel a hozzáférés-kezelésre, a hálózati szegmentációra és a behatolásészlelő rendszerek alkalmazására.
- A régebbi, internetről elérhető ipari vezérlőket – amelyek nem felelnek meg a mai biztonsági elvárásoknak – haladéktalanul válasszák le a nyilvános hálózatokról, ezzel csökkentve a távoli támadások kockázatát.
- Képezze ki az üzemeltető és karbantartó munkatársakat a kiberbiztonsági kockázatok felismerésére, és biztosítsa a kiberbiztonsági tudatosság folyamatos erősítését.
- Kísérjék figyelemmel az NBSZ NKI által közzétett aktuális kiberbiztonsági tájékoztatásokat és riasztásokat a megnövekedett fenyegetettségi helyzetekről.

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Telefon: +36-1-336-4833