Sisemised allikad: Garmin võis maksta küber-väljapressijatele 10 miljonit dollarit teenuste taastamiseks

6 aastat tagasi - 04.08.2020 Autor: AM

23. juulil lakkasid ootamatult Garmini võrku ühendatud nutiseadmed andmeid pilveteenustega sünkimast ning järgnes ülemaailmne Garmini teenuste peatumine. Võisid muidugi sporti edasi teha, kuid tulemusi oma kontole üles laadida polnud võimalik. Mõni päev hiljem küll teenused taastusid, kuid Garmin jäi põhjuste osas kidakeelseks. Mitmete allikate järgi tabas ettevõtet Venemaalt pärit küberkurjategijate rünnak ja et andmed kätte saada, maksti neile vahendajate kaudu 10 miljonit dollarit.

Kõik algas 23. juulil lakoonilisest teatest kasutajate äppides ja seadmetes, et Garmini serverid on ajutiselt maas ja tegemist on vaid kerge hooldusega, "*Check back shortly*" ehk tulge väikese pausi järel tagasi meie teenuseid tarbima.

Paus puudutas Garmin.com ja Garmin Connect teenuseid, sealhulgas klienditeenindust. Veidi hiljem, peale ärevalt pikaks veninud päevade pikkust vaikimist selgus, et probleem tekkis seoses viiruserünnakuga nende süsteemidele.

> In a photo shared with BleepingComputer of an encrypted Garmin computer, you can see that files encrypted during the attack had the .garminwasted extension appended to them.
> pic.twitter.com/mKXKwaC7qS
>
> — BleepingComputer (@BleepinComputer) July 25, 2020

Garmini töötajad nägid arvutites ülalolevat pilti, mis tähendas, et väljapressimistarkvara WastedLocker oli krüpteerinud Garmini tööjaamad. Tavaliselt järgneb sellele lunavaranõue ja kui nõutud summa tasutud, antakse dekrüpteerimisvõti koos programmiga, et oma andmed saaks taastada.

Bleeping Computer sai teada, et lunarahanõue oli 10 miljonit dollarit.

Pärast nelja päeva katkestust teatas Garmin, et teenused hakkavad taastuma, kuid keeldus lunavaranõuet kommenteerimast. Sky News kirjutas, et peale lunaraha tasumist vahendajate kaudu saadi dekrüpteerimisvõtmed ja hakati andmeid taastama.

Küberturbeeksperdid on soovitanud mitte alluda küberkurjategijate väljapressimisele ja soovitavad mitte maksta lunaraha. Samas on väljapressimistarkvara tegutsemine üsna ebameeldiv, kuna isegi varukoopiate tegemisel võib juhtuda, et ka varukoopiad krüpteeritakse samuti ja küberründe puhul pole neist abi.

Kui lunaraha tasumine tõele vastab, siis käitus Garmin vastupidi turvaekspertide soovitustele.

- Uudised
- Turvalisus

Pilt

