Garminit ründas spetsiaalne WastedLockeri Garmini jaoks loodud versioon

5 aastat tagasi - 13.08.2020 Autor: AM

23. juulil langes populaarne trenniseadmete ja GPS-tehnoloogia ettevõte Garmin krüpto-lunavara ründe ohvriks, mis jättis ettevõtte populaarseimad teenused võrguühenduseta kolmeks päevaks, samal ajal kui ettevõtte sisevõrk ja tootmissüsteemid olid krüptitud ja kinni hoitud ilmselt kuni 10 miljoni dollarise lunaraha tasumiseni. See juhtum on uusim suurte rahvusvaheliste ettevõtete vastu suunatud lunavararünnetest. Garminit ründas troojalane WastedLocker — lunavara, mis on selle aasta esimesest poolest aktiivsemaks muutunud. Tehnoloogiaettevõtet tabas versioon, mis oli loodud just Garmini ründamiseks ning sisaldas mitmeid tavatuid lahendusi.

Üheks esimeseks ründevahendiks oli kasutaja pääsureguleerimisest (UAC) möödahiilimise metoodika. Pärast ohustatud seadmes käivitamist kontrollis troojalane, kas sellel on piisavalt ligipääsuõigusi. Kui polnud, proovis tarkvara oma õigusi lisada, pettes süsteemi alternatiivse NTFS-i kaudu käivitama troojalase sisu. Tegemist oli n-ö DLL-faili kaaperdamisega.

Lisaks kasutas Garminit rünnanud WastedLockeri analüüsitud näidis üht avalikku RSA võtit failide krüptimiseks. See oleks nõrk koht, kui pahavara oleks massiliselt levitatud, sest kasutatud lahendusega oleks üht võtit teades saanud kõik nakatunud oma failid lahti dekrüpteerida. Kasutusel oli ainult Garminile suunatud RSA võti. Kui aga rünnak on suunatud ühele ettevõttele, nagu seekord oli, siis polnudki vaja iga kord eraldi privaatset võtit genereerida ning tõhusaks lähenemisviisiks oligi ühe "sissekeevitatud" RSA võtmega lukustamine. Kõik krüpteeritud failid said ümber nimetatud Garminile spetsiifilise laiendiga *.garminwasted.*

Pahavara hoolitses samuti selle eest, et kontrollida dekrüpteerimisel andmete terviklikkust, seega prooviti peale suure lunarahasumma tasumist ikka "kliendile" garanteerida, et kogu info saaks taastatud.

"Garmini juhtum näitab seda, et üha enam tekib krüpto-lunavara ründeid konkreetsete suurettevõtete vastu — vastupidiselt minevikus levinumatele ja populaarsematele lunavaraprogrammidele, nagu WannaCry ja NotPetya. Ehkki ohvreid on vähem, on sellised suunatud rünnakud tavaliselt keerukamad ja hävitavamad. Puuduvad tõendid, mis viitaksid sellele, et lähitulevikus nende arv väheneb. Seetõttu on kriitilise tähtsusega, et asutused jääksid valvsaks ja astuksid samme enda kaitsmiseks," kommenteeris lunavararünnakut uurinud Kaspersky turbeekspert Fedor Sinitsyn.

Lisateavet ja tehnilisemaid kirjeldusi Garmini vastu suunatud WastedLockeri ründe kohta saab siit.

WastedLockeri ja muu lunavaraga kokkupuuteohu vähendamiseks soovitavad Kaspersky eksperdid:

1. Kasuta operatsioonisüsteemi ja rakenduste ajakohaseid (uusimaid) versioone
2. Kasuta VPN-i ettevõtte ressurssidele kaugjuurdepääsu tagamiseks
3. Kasuta tänapäevaseid lõpp-punkti turbelahendusi koos tarkvara kahtlase käitumise tuvastustoe ja parandamismootoriga, mis võimaldab faili automaatset tagasipööramist
4. Täienda töötajate küberturbealast haridust
5. Kasuta usaldusväärset (mitmetasemelist) andmevarundusskeemi või -lahendust

- Uudised

- Tarkvara
- Turvalisus

Pilt