

ACPM IT Tanácsadó Zrt.

Szoftver ellátási láncot érintő biztonsági kockázatok

Debreceni Egyetem Informatikai Kar - EIVOK-30. Tudományos - Szakmai Konferencia
2022. november 4.

Miről lesz szó?



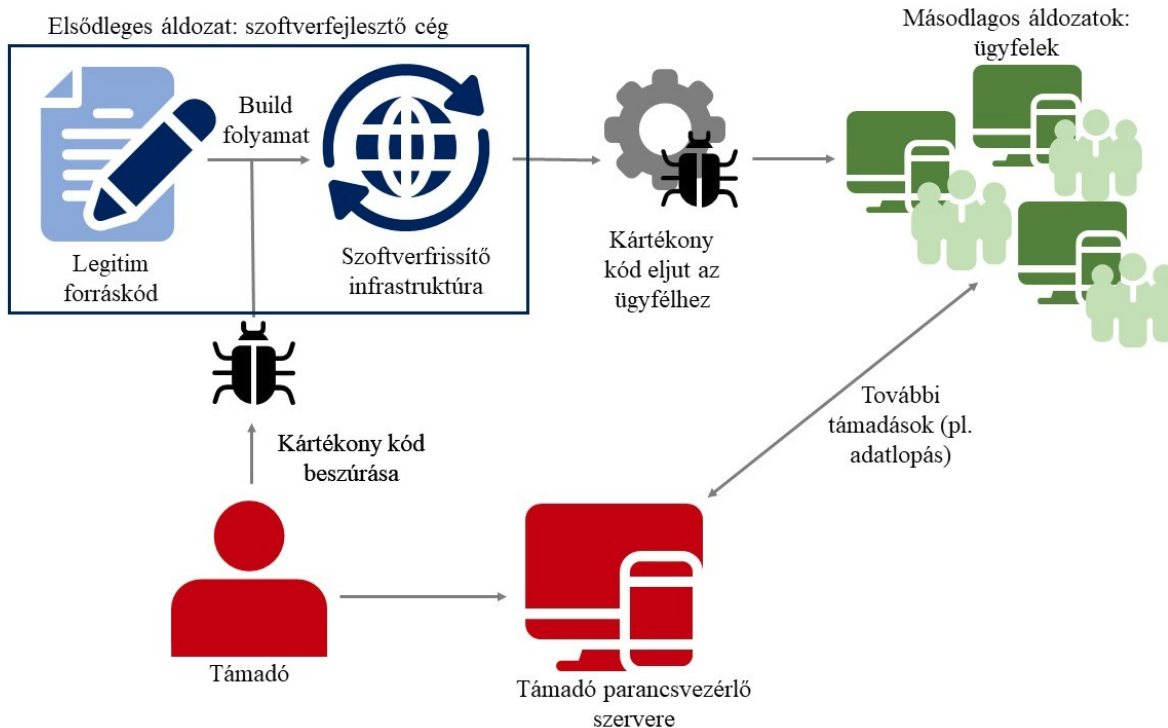
- Szoftver ellátási lánc sajátosságai
- Korábbi emlékezetes incidensek
- További témába vágó problémák
- Javaslatok, gondolkodás a megoldás irányába

Szoftver ellátási lánc sajátosságai



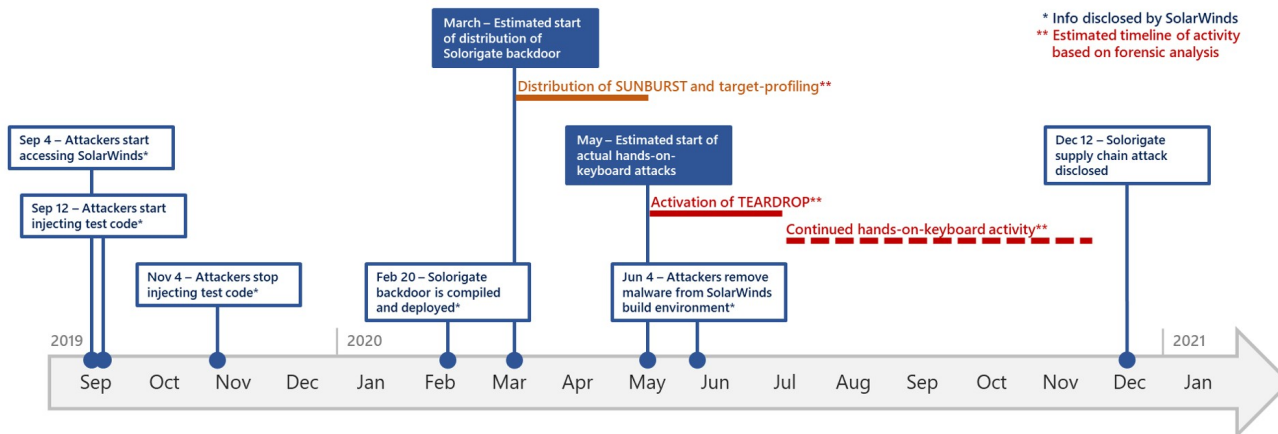
- A termék eredete akár bonyolultabb lehet, mint a fizikai termékek esetében. / Honnan van az alkatrész?
- A fejlesztés mögötti folyamatok is bonyolultabbak lehetnek, mint a fizikai gyártásban
- Kiesés / probléma esetén (szintén) nagyon nehéz pótolni / cserélni
- Kritikus infrastruktúra-e a szoftverfejlesztés?

Szoftver ellátási lánc támadása



Korábbi incidensek 1


- 2021. február Franciaország **Cetreon**; ~600 érintett ~2 év
- 2020 Solarwinds Orion / Fireeye érintettség külön téma ...
- Dráma több felvonásban



Korábbi incidensek 2

- 
- 2015.12.17. Juniper ScreenOS
 - 2016 Fortinet
 - 2013. EMC / RSA : Dual_EC_DRBG algoritmus
 - 2014 Yulong Coolpad gyári 2012. ZTE hálózati eszköz frissítés

Más típusú kockázatok

- 
- 2021. január MS Exchange 0 day ~30.000 érintett
 - 3rd party alkalmazások
 - Konténerek
 - 2019-2020 ~legalább 18.000 érintett (vagy több)

▶ Mit kellene / lehetne tenni?

- Common Criteria jó lehetne, DE ...
- Az alkalmazott eszközök nem lehetnek fekete dobozok!
- Szoftver, illetve rendszer akkreditációk, minősítések ...
- Fejlesztők és üzemeltetők biztonság tudatosságának fejlesztése, szakértői biztonsági minősítések ...
- Szervezet, illetve cég akkreditációk, minősítések ...
- (ágazati) bevezetése, ezek elterjedésének megkövetelése!
- **A kibertérben támadóelőny van!**

▶ Szoftvereket használni kockázatos !



Köszönöm a figyelmet!

ACPM IT Tanácsadó Zrt.

Széchenyi István tér 7-8.
Budapest, 1051
www.acpmit.com