Útoky supply chain: Případ SolarWinds

Jiří Gogela
Trend Micro Research - DVlabs Praha

Co je Supply Chain útok

Wikipeda: *„...in reference to cyber-security, a supply chain attack involves physically tampering with electronics (computers, ATMs, power systems, factory data networks) in order to install undetectable malware for the purpose of bringing harm to a player further down the supply chain network.“*

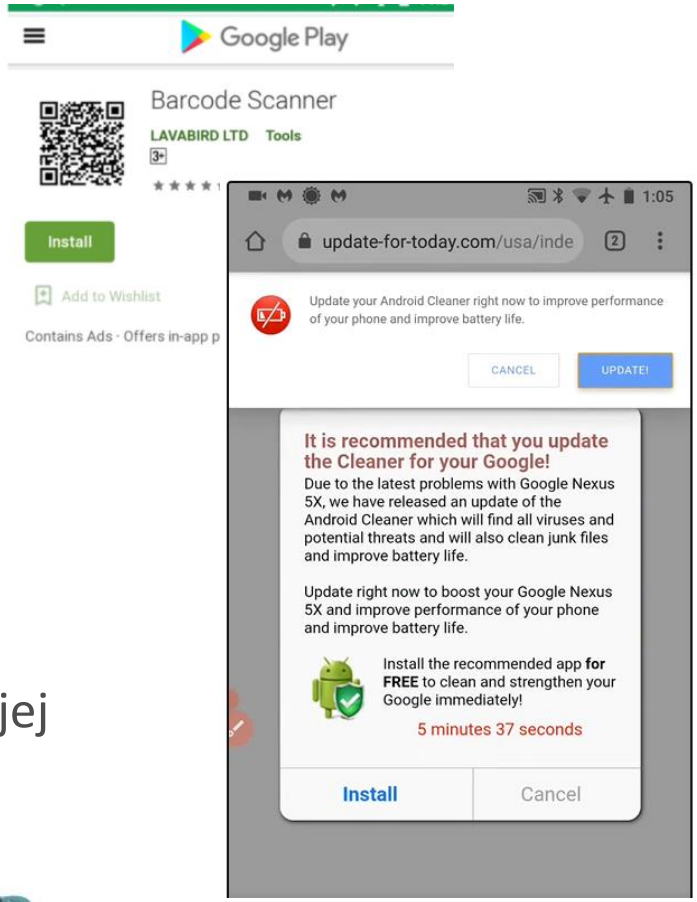
V softwarovém vývoji je za supply chain považováno použití software třetích stran. Ať už samostatně nebo jako komponenty vlastního řešení.

Za supply chain útok tak bývá považována situace, kdy si malware přinesete do svého systému jako součást oficiálního (někdy i draze placeného) software.

Případ 1: Lavabird

Barcode Scanner od Lavabird ltd

- Na Google play dostupný už několik let
- Více než 10M stažení
- V prosinci 2020 vyšel update obsahující závadný kód, který zaplavoval uživatele pochybnou reklamou.
- Podle dostupných informací původní vývojové studio prodalo software včetně práv k účtu na Google Play a nový majitel jej využil k šíření malware.
- Google aplikaci v řádu dnů stáhl z GPlay



Případ 2: SolarWinds (Sunburst, Solorigate)

Jedním z největších případů supply-chain útoku poslední doby je zneužití systému Orion dodávaného firmou SolarWinds

SolarWinds
- Americká softwarová firma
- Založeno 1999
- 3200 zaměstnanců (velké vývojové středisko v Brně)

Orion
- Systém pro správu podnikových sítí
- 33000 zákazníků, především velké firmy a státní instituce.

Co se přihodilo?

- V prosinci 2020 byl odhalen rozsáhlý kybernetický útok na celou řadu soukromých i vládních organizací.
- Útočníci byli schopni proniknout do systému vyvoje firmy SolarWinds a modifikovat software tak, aby útočníkům umožňoval vzdálený přístup (backdoor).
- Tato úprava byla zveřejněna jako aktualizace software.
- Zhruba 18000 zákazníků si tuto závadnou verzi stáhlo.
- Řada z těchto zákazníků byla následně napadena.

Postup útoku a jeho odhalení

Září 2019, pravděpodobný průnik do systému SolarWinds

Říjen 2019 první modifikace zdrojového kódu Orion

6.12. Registrace domén použitých v útoku

Únor – vytvoření SSL certifikátu

Březen-červen 2020 Publikování závadných aktualizací pro SW Orion

8.12. FireEye: oznámení o úniku nástrojů pro pentesting

? FireEye: 2FA incdent

13.12.Oznámení DHS

15.12.Zablokování domén sloužících k útoku

13.12. FireEye: detekce malware Sunburst v produktech Solarwinds

2019

2020

Postižené instituce (částečný seznam)

- Cybersecurity - CrowdStrike, Fidelis, FireEye, Malwarebytes, Palo Alto Networks, Qualys
- IT -Microsoft, Belkin, Cisco, Intel,Nvidia, VMware
- Consulting - Deloitte
- US govt - Dept. of Energy, Dept. of Commerce, Dept. of Health, Dept. Of Homeland Security, Pentagon, State Department, Treasury Dept.

Co vlastně víme?

- Stále není jasné jak útočníci pronikli do systému Solarwinds.
- Útočníci se zřejmě pohybovali v napadených systémech několik měsíců, dosud není jasné co si odnesli, či naopak co dalšího tam mohli přinést.
- Odhalení přinesla víceméně náhoda.
- SolarWinds doporučoval pro instalaci vypínat antivirus
- Akce byla velmi dobře propracovaná a necílila na okamžitý profit.
- Microsoft odhaduje, že na přípravě útoku muselo pracovat více než 1000 lidí (!)

TREND MICRO™

THE ART OF CYBERSECURITY

Threats detected and blocked globally by Trend Micro in 2018. **Created with real data by artist Daniel Beauchamp.**