#### Secureworks

### Solorigate / Sunburst

Tonttu-koulutus 11.6.2021

#### Kuka?

- Dr. Nestori Syynimaa
- Vanhempi tietoturvatutkija @ Secureworks
- AADInternals työkalun kehittäjä

#### Yhteystiedot

- nsyynimaa@secureworks.com
- Twitter: <a>@DrAzureAD</a>
- <a href="https://linkedin.com/in/nestori">https://linkedin.com/in/nestori</a>
- https://o365blog.com













#### Sisältö

- Mikä ihmeen Solorigate hyökkäys?
- Miten hyökkäys organisaation pilveen tehtiin?
- Suojaus- ja varautumistoimet
- Korjaustoimenpiteet

# Mikä Solorigate hyökkäys?

#### Solorigate / Sunburst hyökkäys

- "Toimitusketju hyökkäyksen" avulla SolarWinds yrityksen Orion valvontaohjelmistoon tehty takaportti
  - Ensimmäiset havainnot syyskuulta 2019, KTK:n julkaisu 18.12.2020
  - Kohdistui jopa 18 000 asiakkaaseen
  - Mahdollisti pääsyn organisaation sisäverkkoon ja palvelinympäristöön
  - Mahdollisti pääsyn organisaation Office/Microsoft 365 ympäristöön

# Miten hyökkäys organisaation pilveen tehtiin?

#### Pilveen kytketyt palvelut

- Azure AD Connect
  - Tietojen synkronointi oma ympäristö → pilvi
  - Objektit (käyttäjät, ryhmät, kontaktit, laitteet) (ja salasanatiivisteet)
  - Laajat luku- ja kirjoitusoikeudet Azure AD ja AD
- Active Directory Federation Service (AD FS)
  - Käyttäjien federoitu tunnistaminen
  - Kertakirjautuminen (SAML)
- Seamless Single-Sign-On
  - Kertakirjautuminen (Kerberos)

#### **Azure AD Connect**

Kolme käyttäjätunnusta:

Tunnus	Käyttöoikeudet
Sync_xxx_yyy@zzz.onmicrosoft.com	<ul><li>Azure AD tunnus, jolla tietoja synkronoidaan</li><li>Kaikki normaalin käyttäjän oikeudet</li><li>Oikeudet lisätä/muokata/poistaa käyttäjiä</li></ul>
DOMAIN\MSOL_yyy	<ul><li>AD tunnus, jolla tietoja synkronoidaan</li><li>Lukuoikeus koko hakemistoon</li><li>AD replikointioikeus</li></ul>
DOMAIN\AAD_yyy	<ul><li>Palvelutunnus, jolla synkronointipalvelua ajetaan</li><li>Ei oikeuksia hakemistoihin</li><li>Käyttää edellisiä</li></ul>

- Tunnukset tallennettu Azure AD Connect koneelle
- Tunnusten lukemiseen riittää paikallisen järjestelmänvalvojan oikeudet

#### **Active Directory Federation Service (AD FS)**

- Federoitu tunnistautuminen
  - Tunnistautuminen omaa AD:ta vasten
  - Ei salasanoja pilvessä
- Perustuu (Azure AD ↔ AD FS) luottosuhteeseen
  - AD FS palvelun allekirjoitusvarmenteen julkinen avain AD:ssa (max. 2 kpl)
  - AD FS tunnistaa käyttäjän, muodostaa SAML tokenin ja allekirjoittaa sen
- Varmenteen suojaus
  - Varmenne salattuna konfiguraatiotietokannassa (paikallinen tai SQL)
  - Salausavain tallennettu AD objektiin

#### **Seamless Single-Sign-On**

- Perustuu Kerberos tunnistautumiseen
- AZUREADSSOACC konetili
  - Luodaan SSSO käyttöönotossa
  - Salasanatiiviste Azure AD:ssa
  - Yhdistetty palvelunimeen <a href="https://autologon.microsoftazuread-sso.com">https://autologon.microsoftazuread-sso.com</a>
- Luottosuhde
  - Kerberos tiketit salataan ja allekirjoitetaan konetilin salasanalla

#### Yhteenveto hyökkäystavoista

- Azure AD Connect palvelin
  - Pääsy synkronointitunnuksiin paikallisen koneen pääkäyttäjänä
  - Mahdollistaa käyttäjien luonnin, muokkauksen ja poiston pilveen
  - Mahdollistaa pääsyn AD käyttäjien salasanatiivisteisiin

#### AD FS

- Pääsy allekirjoitusvarmenteeseen (paikallinen pääkäyttäjä) ja sen salausavaimeen (domain admin, AD FS palvelutunnus, tai replikointioikeus)
- Mahdollistaa kirjautumisen pilveen kenä tahansa käyttäjänä (MFA ohitus)

#### SSSO

Mahdollistaa kirjautumisen pilveen kenä tahansa käyttäjänä

# Suojaus- ja varautumistoimet

#### Oma ympäristö

- Suojaa KAIKKI pilveen kytketyt järjestelmät yhtä hyvin kuin Domain Controllerit (AD:t)
- Azure AD Connect
  - Monitoroi tietokannan (poikkeuksellista) käyttöä
- AD FS
  - Monitoroi salausavaimen lukua
  - Rajoita 80 porttiin (http) tuleva liikenne vain AD FS ja proxy palvelinten väliseksi
- SSSO
  - Kierrätä säännöllisesti AZUREADSSOACC ja KRBTGT konetilien salasanat

#### Pilvi

- Monitoroi kaikkia domaineihin liittyviä muutoksia
- Monitoroi kaikkia sovelluksiin (apps) liittyviä muutoksia
- Minimoi Global Administrator tunnusten lukumäärä
- Käytä monen tekijän tunnistautumista (MFA)
- Rajaa Azure AD Connect tunnuksen kirjautuminen määrättyyn ip-osoitteeseen

## Korjaustoimenpiteet

#### Oma ympäristö

- Azure AD Connect
  - Resetoi tunnukset (ei tuettu) tai asenna uudelleen, ja poista vanhojen tunnusten oikeudet
- AD FS
  - Kierrätä allekirjoitusvarmenne kahteen kertaan
- SSSO
  - Kierrätä AZUREADSSOACC ja KRBTGT konetilien salasanat kahteen kertaan

#### Pilvi

- Ota talteen kaikki mahdolliset kirjautumis- ja auditointilogit
- Federoidut toimialueet (domainit):
  - Tarkista tiedot tai muodosta luottosuhteet uudelleen
- Sovellukset
  - Tarkista tunnistautumistiedot tai poista ja asenna uudelleen
- Tarkista hallintaroolien jäsenyydet

## Lopuksi

#### Tee ainakin nämä

- Suojaa kaikki pilveen kytketyt järjestelmät
- Minimoi pääkäyttäjäoikeudet
- Käytä MFA:ta
- Tallenna logitiedot säännöllisesti