PLAYBOOK ÎN CONTEXTUL ATACULUI DE TIP SUPPLY CHAIN VIA SOLARWINDS ORION

În ultimele zile, comunitatea de cybersecurity a fost alertată în privința unui **atac cibernetic de tip supply chain** prin actualizările furnizate de compania **SolarWinds** pentru **SolarWinds Orion**.

VEZI MAI MULTE DETALII AICI

Acesta este unul dintre cele mai periculoase scenarii pentru multe organizații: un actor avansat sponsorizat de un stat poate să fi avut deja acces la infrastructurile organizației dumneavoastră timp de mai multe luni, printr-un backdoor nedetectat.

Drept urmare, specialiști în domeniu au început documentarea problemei, iar unul dintre pașii pentru remediere implică acțiuni strict necesare pentru a izola, eradica și remedia backdoorul de la SolarWinds.

Având în vedere pericolul generat de un astfel de atac pentru infrastructuri (rețele și sisteme) informatice, echipa CERT-RO vă pune la dispoziție un ghid de acțiuni recomandate (playbook).

Este recomandat să presupunem infrastructurile dumneavoastră au fost deja compromise ca urmare a atacului. Prezentul ghid operează pe baza acestei presupuneri.

INVESTIGARE → IZOLARE → ELIMINARE → RECUPERARE

- Chiar dacă ați efectuat deja măsuri de răspuns, recomandăm parcurgerea pașilor acestei liste. Pot exista aspecte pe care nu le-ati avut în vedere.
- Fiecare organizație trebuie să determine efectele acțiunilor de remediere propuse și să se asigure că efectele sunt acceptabile pentru organizație.

INVESTIGARE

Investigarea ar trebui să aibă loc simultan cu izolarea și stoparea atacului precum și cu procesele de recuperare. Serverele SolarWinds Orion ar trebui să fie conservate pentru a permite o examinare ulterioară de tip „forensic”. Aceasta include:

- Obținerea de live response data, inclusiv RAM
- Imaginea și hashingul disk-ului
- Salvarea network log-urilor (ex. Firewall, NetFlow) serverelor, înainte de a fi rulate
- Exportarea log-urilor centralizate, înainte ca serverele să fie rulate

Având în vedere că vizibilitatea internă este diferită la fiecare organizație, am compus o listă de întrebări la care să răspundeți pentru perioada în care organizația dvs. a avut SolarWinds Orion implementat, începând din martie 2020. Pentru întrebările la care nu există un răspuns, organizațiile ar trebui să identifice o soluție viitoare.

ACTIVITATEA UTILIZATORILOR

Printre conturile menționate mai jos sunt incluse atât conturi utilizate de SolarWinds (ca furnizor), pentru a realiza monitorizarea și managementul, stocate pe infrastructura SolarWinds, cât și conturi locale din cadrul serverelor Orion.

- S-au autentificat acele conturi (cu succes sau nu) la sisteme sau aplicații la care nu ar trebui să aibă acces? Dacă nu aveți log-uri atât de vechi, va trebui să realizați o căutare la nivelul log-urilor stocate local în mediul dumneavoastră.
- Au primit acele conturi încercări de autentificare (cu succes sau nu) din locații externe, în special din unele din care să nu se fi logat înainte (ex. prin VPN)?
- Au dezactivat acele conturi alertele „impossible travel”?
- Există aplicații OAUTH suspicioase ce permit Mail.Read sau Mail.ReadWrite (sau permisiuni excesive) în cadrul Office365?

ACTIVITATEA DIN REȚEA

- Există sisteme conectate la domeniile de comandă și control (C2) sau adrese de IP cunoscute?
- Există sisteme conectate la adresa de IP DNS sinkhhole (20.140.0.1)?
- Există servere conectate la domenii sau adrese IP externe?
- Există servere conectate la sisteme interne la care nu ar trebui să fie conectate?
- Există servere conectate la sisteme interne în momente sau zile în care nu ar trebui să existe astfel de conexiuni?
- Există noi „federation trusts” adăugate la Azure tenants existente?

ACTIVITATEA ENDPOINT

- Este backdoor-ul Dynamic-Link Library (DLL) încă prezent pe serverele Orion?
- Există backdoor-ul DLL pe vreun alt server? (Indiciu: Utilizați semnăturile sau hash-urile FireEye Yara ale DLL-urilor pentru căutări)
- Există vreun indiciu de activitate suspicioasă pe serverele Orion?
- Există activitate suspicioasă pe sistemele/aplicațiile cu date stocate pe serverele Orion?
- Există ASEP-uri suspicioase pe servere sau software-urile pentru acces de la distanță?
- Există conturi adăugate sau reautorizate pe serverele Orion sau alte sisteme sau aplicații la nivelul cărora Orion avea acces de administrare?
- Au fost validate toate fișierele pentru configurarea dispozitivelor la care Orion avea acces?
- Au detectat software-urile de securitate (anti-virus, Endpoint Detection and Respons (EDR)) activitate suspicioasă sau malware în cadrul sistemelor?

ACTIVITATEA POST-EXPLOIT

- A fost detectată activitate post-exploit pe vreun sistem?
- Rapoartele FireEye susțin că a fost utilizat un payload de exploatare CobaltStrike.

  Vezi: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
- Fișierele cunoscute includ c:\windows\syswow64\netsetupsvc.dll
- Există certificate RDP SSL ale organizației publicate online? (Indiciu: verificați Shodan)

IZOLARE

În acest subcapitol primiți recomandări cu privire la stoparea răspândirii atacului sau prevenirea unor daune ulterioare cauzate de atac.

CARANTINAȚI SERVERELE SOLARWINDS ORION care au backdoor DLL, astfel încât să nu poată comunica cu nicio altă rețea sau sistem. Opțiuni posibile:

- Rutare NULL a adreselor IP în cauză.
- Plasarea serverelor Orion într-o rețea proprie separată, fără acces la alte sisteme sau la internet.
- Utilizarea EDR pentru a izola sistemele.
- Oprirea serverelor. Dacă mergeți pe această idee, asigurați-vă că ați preluat mai întâi datele de forensics cu răspuns live - este mai bine să le aveți și să nu aveți nevoie de ele.

DEZACTIVAȚI ORICE CONTURI UTILIZATE DE SOLARWINDS ORION pentru a accesa alte dispozitive sau pentru a comunica în rețeaua dvs. Acestea includ:

- Contul de service-are al platformei Orion
- Contul SQL database service
- Orice cont utilizat pentru monitorizarea aplicațiilor/sistemului/WMI de la Orion
- Conturi utilizate de Orion pentru a trimite alerte
- SNMP community strings

BLOCAȚI COMUNICAREA REȚELEI CU DOMENIILE C2 ȘI ADRESELE IP CUNOSCUTE, pentru toate sistemele. Opțiunile posibile includ:

- Domenii sinkhole DNS
- Blocați adresele IP la firewall-uri
- Blocați domeniile și adresele IP din serverele proxy
- Porniți semnăturile IPS legate de Sunburst

BLOCAȚI ACCESUL LA INTERNET PENTRU SERVERELE SOLARWINDS ORION.

CONFIGURAȚI ALERTAREA pentru orice sistem care accesează indicatorii de compromis (IoC) cunoscuți pentru Sunburst sau utilizarea oricărui ID de utilizator care a fost dezactivat. Acest lucru ar trebui făcut atât pentru monitorizarea endpoint, cât și pentru rețea.

ELIMINARE

Eradicarea este procesul de eliminare a unui atacator sau a unui sistem afectat dintr-un mediu.

- Schimbați parolele pentru orice cont utilizat de SolarWinds Orion. Utilizatorul *sturdyerde* a postat recent o metodă excelentă pentru a face acest lucru, pe forumul comunității SolarWinds.

  Vezi: https://thwack.solarwinds.com/t5/NPM-Discussions/When-you-have-to-change-all-passwords-for-the-Orion-monitoring/td-p/613340
- Schimbați toate parolele partajate pentru conturile care erau pe serverele SolarWinds Orion. Aceast proces include parole de cont locale partajate sau conturi de servisare de pe sistem.
- Schimbați parolele sau community strings stocate în Orion pentru a efectua monitorizarea.

- Dacă acest lucru nu a fost făcut în faza de izolare, eliminați serverele Orion din rețea.

Rețineți că, în loc să modificați parolele pentru conturi, pote fi mai rapid și mai ușor să creați conturi noi și să eliminați vechile conturi utilizate în și de SolarWinds Orion.

RECUPERARE

Recuperarea se referă la procesul de a readuce sistemele la operațiuni normale.

- Faceți backup pentru configurația și baza de date SolarWinds. Informații despre acest lucru găsiți în documentația SolarWinds Orion.
- Reconstruiți sistemul de operare dintr-o imagine anterioară.
- Instalați SolarWinds versiunea 2020.2.1 HF 2

  Vezi: https://www.solarwinds.com/securityadvisory
- Asigurați securitatea și vizibilitatea endpoint-urilor pe server.
- Recuperați datele din back-up-ul configurației și al bazei de date.
- Verificați hashurile criptografice ale fișierului SolarWinds.Orion.Core.BusinessLayer.dll instalat, pentru a vă asigura că backdoor-ul DLL nu mai este prezent. Hash-urile pot fi găsite în ghidul Microsoft pentru clienți.

Alternativ, este posibil ca reconstruirea completă a serverului de la zero să nu fie fezabilă, deși aceasta este metoda preferată și recomandată. Dacă nu puteți face acest lucru, efectuați următoarele acțiuni:

- Faceți backup pentru configurația și baza de date SolarWinds.
- Instalați remedierea rapidă pentru SolarWinds Orion 2020.2.1 HF 2.
- Asigurați securitatea și vizibilitatea endpoint-urilor în servere.
- Verificați hashurile criptografice ale fișierului SolarWinds.Orion.Core.BusinessLayer.dll instalat, pentru a vă asigura că backdoor-ul DLL nu mai este prezent.

Dacă preferați abordarea de restaurare față de abordarea de reconstrucție, trebuie totuși să efectuați proceduri de izolare și eradicare!

Indiferent de abordarea adoptată, trebuie să faceți următoarele activități de recuperare:

- Eliminați toate măsurile de izolare temporare care au fost puse în aplicare.
- Asigurați-vă că alertele pentru rețea și endpoint sunt configurate pentru următoarele:
  - Prezența oricărui IoC cunoscut
  - Utilizarea conturilor într-un mod suspect (de exemplu, un cont de serviciu SolarWinds care încearcă să se conecteze la VPN)
- Asigurați-vă că software-ul de securitate a rețelei și a endpoint-urilor este actualizat în ceea ce privește semnăturile, inclusiv cele legate de Sunburst.

Aveți suspiciuni că organizația dumneavoastră a fost compromisă de atacul SolarWinds Orion?

alerts@cert.ro www.cert.ro Tel: 1911