La password per i server di SolarWinds era in chiaro su GitHub

Dic 16, 2020 Marco Schiaffino Attacchi, Gestione dati, Hacking, In evidenza, Intrusione, Leaks, Malware, News, RSS, Vulnerabilità 0

Nessuna certezza sul fatto che sia stata usata per l'attacco che ha colpito l'azienda informatica, ma il livello della sicurezza era ridicolo.

Mentre gli esperti di cyber security si danno da fare per capire quali siano i reali contorni dell'attacco hacker che ha preso di mira decine (migliaia?) tra aziende ed enti pubblici, emergono nuovi dettagli sulle modalità con cui i pirati informatici potrebbero aver avuto accesso ai sistemi di **SolarWinds**.

L'azienda texana, come abbiamo spiegato in questo articolo, è all'origine dell'attacco supply chain che ha permesso ai cyber criminali di inserire il trojan **SUNBURST** all'interno degli aggiornamenti di **Orion**, il suo software per la gestione delle infrastrutture IT che sarebbe stato scaricato da 33.000 tra aziende e istituzioni in tutto il mondo.

Ora emergono dettagli su alcuni "piccoli difetti" nei sistemi di sicurezza di SolarWinds, che potrebbero spiegare come sia stato possibile per i pirati introdursi nei suoi sistemi.

A riportarlo è **Vinoth Kumar**, un ricercatore che nel novembre 2019 ha segnalato agli amministratori dell'azienda che in un repository su **GitHub** erano accessibili **username e password** per il server FTP in cui sono memorizzati gli installer di Orion.

Come se non bastasse, il ricercatore fa notare che la password per l’accesso al servizio di upload degli eseguibili non era proprio aderente alle best practice in tema di credenziali: era infatti “**solarwinds123**”. Qualcosa che avrebbe potuto indovinare un bambino di 7 anni.

Possibile che i pirati abbiano utilizzato questa password per portare l’attacco? Beh, da un punto di vista cronologico i conti tornano. **Secondo Kumar, le credenziali erano accessibili su GitHub già nel giugno 2018**.

La prima versione di Orion contenente il malware (2019.4) è stata distribuita da SolarWinds il 5 novembre 2019, **due settimane dopo la segnalazione di Kumar**.

Insomma: non c’è nessuna certezza, ma è possibile che il più grande attacco hacker degli ultimi 5 anni abbia avuto origine da un errore di configurazione e un banale leak a livello di documentazione.

Condividi l’articolo

Terzo data breach per Spotify. Cambio di password per gli utenti coinvolti

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/12/16/la-password-per-i-server-di-solarwinds-era-in-chiaro-su-github/?utm_source=rss&utm_medium=rss&utm_campaign=la-password-per-i-server-di-solarwinds-era-in-chiaro-su-github