L’azienda di sicurezza informatica Malwarebytes è stata violata dagli hacker di SolarWinds

Lo stesso gruppo che ha violato la società di software IT **SolarWinds** lo scorso dicembre ha violato la società di sicurezza informatica americana **Malwarebytes**.

Lo riporta la stessa azienda californiana in un post scritto dal CEO dell’azienda di cybersecurity **Marcin Kleczynski**.

“Malwarebytes ha appreso della violazione il 15 dicembre dal Microsoft Security Response Center e da allora ha indagato sulla questione”, scrive il CEO. *“I Criminali informatici hanno avuto accesso solo ad un numero limitato di e-mail aziendali interne*“, aggiungendo che *“il software dell’azienda resta sicuro da usare”.*

Malwarebytes ha affermato che gli hacker hanno utilizzato una debolezza in **Azure Active Directory** e applicazioni dannose di **Microsoft Office 365** per violare i sistemi interni dell’azienda. Inoltre l’hackeraggio non è correlato alla violazione dei software SolarWinds, poiché Malwarebytes non utilizza nessuno dei loro sistemi.

SolarWinds: cosa è successo

Lo scorso 13 dicembre i media statunitensi hanno diffuso la notizia del “*più grave attacco informatico da cinque anni a questa parte agli Stati Uniti” che ha coinvolto l’amministrazione Usa.* I cyber attacchi, legati si pensa ai

servizi segreti russi con il gruppo APT29 "*Cozy Bear*", hanno colpito il Dipartimento del Tesoro e il Dipartimento del Commercio, più altre Agenzie governative di massimo rilievo istituzionale tra cui l'Agenzia per la sicurezza nucleare degli Stati Uniti.

La breccia nel sistema di difesa è stata individuata in alcuni software della **NTIA**, la National Telecommunications and Information Administration, in particolare in **Microsoft Office 365**, superando il sistema di autenticazione. Ma la falla più grave è stata individuata dagli investigatori americaninegli aggiornamenti software rilasciati dalla società informatica texana **SolarWinds**, che fornisce servizi ad agenzie governative e Dipartimenti del Governo, nonché all'intelligence USA e ai militari.

> *Today, I disclosed publicly that @Malwarebytes had been targeted by the same nation state actor that attacked SolarWinds. This attack is much broader than SolarWinds and I expect more companies will come forward soon.*
>
> *— Marcin Kleczynski (@mkleczynski) January 19, 2021*

In un messaggio pubblicato su Twitter, **Kleczynski** ha affermato che la campagna di hacking che ha coinvolto SolarWinds "*è molto più ampia e mi aspetto che altre aziende si facciano avanti presto*".

https://www.key4biz.it/lazienda-di-sicurezza-informatica-malwarebytes-e-stata-violata-dagli-hacker-di-solarwinds/340352/