AlphV claims an attack before even alerting the victim. How will that work out for them? (1) - DataBreaches.Net

Published: 2023-12-03 · Archived: 2026-04-09 02:08:08 UTC

So AlphV (aka BlackCat) is trying something different again, it seems.

 This time, it seems they are claiming a victim before they have even attempted to contact the victim or extort them. They post no proof of claims. They state that they are taking this approach because the victim's cyberinsurance policy does not cover extortion, and their research into the victim (Tipalti) and one of the victim's clients (Roblox) suggests that their usual approach will not work. They intend to try to extort those firms and Twitch, all individually. Tipalti is an accounting software financial technology business that provides accounts payable, procurement and global payments automation software for businesses.

AlphV's listing states, in part:

> We have remained present, undetected, in multiple Tipali systems since September 8th 2023. Over 265GB+ of confidential business data belonging to the company, as well as its employees and clients has been exfiltrated. We remain committed to this exfiltration operation, so we plan to reach out to both these companies once the market opens on Monday as we believe we will have an even greater amount of data by then, in addition to the likely inability of the Tipali company to be able to contain our efforts by then, given their incompetency and taking into account that an insider was , and is still actively involved. This article will be republished on Monday just before the market opens, to maximize the impact to the $RBLX stock price.

This listing is not the very nasty approach that we've seen in some other listings on that leak site, although there is a mention of "filthy criminals." The claim that an insider is involved is noteworthy. Whether it is true or not is not something we are not likely to find out quickly, and it may just be a false claim made to make the firm doubt themselves and their own internal resources.

AlphV's full listing also cites an academic reference on the potential benefit of paying ransom. It is not clear for whose benefit they have included that citation, but it's interesting that they spend any time finding or including such material.

DataBreaches has sent an email inquiry to Tipalti, but no reply was immediately received. This post will be updated when they respond or issue a statement. For now, DataBreaches reminds readers that AlphV's claims are unconfirmed.

Update 1: DataBreaches has not yet received any reply from Tipalti, but a reader kindly sent us a link to an Israeli news source that did obtain a statement from them:

> מטיפלתי נמסר: "אנחנו מכירים את הטענה הזו וחוקרים אותה. אנחנו לוקחים בכל החומרה והחשיבות את בטחון מידע לקוחותינו. נכון לרגע זה לא זיהינו כל אובדן מידע או פריצה למערכות שלנו".

In Yandex translation:

> A spokesman said: "We are aware of this allegation and are investigating it. We take the security of our customers' information with the utmost seriousness and importance. At this time, we have not detected any data loss or breach of our systems."

Source: https://www.databreaches.net/alphv-claims-an-attack-before-even-alerting-the-victim-how-will-that-work-out-for-them/