Dropbox Suffers Major Breach
In Phishing Attack

It's no secret that cyber attacks are on the rise, and that no company is immune to them. Dropbox, a cloud storage company, was the lastest victim when their GitHub account was compromised. This allowed attackers access to 130 code repositories, which contained sensitive data.

Dropbox was notified of a potential breach on October 14th from GitHub, who observed suspicious activity coming from the account starting one day earlier.

On Tuesday, November 1, 2022, Dropbox released an announcement that said, "our investigation has found that the code accessed by this threat actor contained some credentials—primarily, API keys—used by Dropbox developers." The data contains the names and email addresses of a few thousand Dropbox employees, current customers, past customers, sales leads, and vendors.

A successful email phishing campaign, targeting Dropbox employees and pretending to be from CircleCI (a continuous integration and delivery platform), has been attributed to a recent data breach. The emails directed the victims to a landing page where they were asked to enter their GitHub credentials.

Dropbox states that the hackers did not manage to get access to customers' accounts, passwords, or payment information. In addition, none of Dropbox's core apps or infrastructure were compromised. As a result of this attack, Dropbox is taking further steps to secure its environment by using WebAuthn and hardware tokens or biometrics.

It was almost immediately after the compromise that GitHub detected the exfiltration of content from private repositories. The threat actors used VPNs and proxy services to make it more difficult to trace and identify them.

The Dropbox security breach is just one example of how even big companies are susceptible to damage by sophisticated cyber attacks. But while Dropbox was quick to mitigate the damage caused by the attack, it's a reminder to all businesses that they're always vulnerable to these kinds of threats. Therefore, it's important for employers educate their staff on how identify potential cyberattacks.

IT Professional Say Business VPN Attacks Are On The Rise

IT professionals are seeing an increase in exploits targeting their VPNs, a report jointly-authored by two cybersecurity firms has found.

Business VPNs remain a popular way to provide secure access to company servers from remote locations, but other, more secure ways to construct secure network infrastructure are emerging. Are VPNs done for? Probably not just yet, but novel ways to facilitate secure access to company networks are certainly becoming more common.

According to the 2022 VPN Risk Report carried out by Cybersecurity Insiders and Zscaler, 44% of cybersecurity professionals witnessed an "increase in exploits targeting their VPNs".

It's not surprising either, considering the size of the attack surface – 61% of companies have three or more VPN gateways, and 38% have more than five. The more gateways you have, the more complex and ultimately expensive your network architecture is to maintain.

The survey also found that 71% of cybersecurity professionals are "concerned that VPN may jeopardize the ability to keep the environment secure".

VPNs Aren't Impenetrable

In essence, business VPNs extend company networks, in order to let people in various locations access sensitive resources. But this also means that if the network is insecure, there are more ways a hacker can access and subsequently exploit it. VPNs also can't really do anything about a malware-infected device on a company network.

Plus, the way VPNs encrypt traffic (it is encrypted between two objects connected to the network, such as a server and a device) means that a full, distinct security stack has to be deployed at every endpoint to inspect traffic, which is a resource-heavy activity.

What's more, VPN credentials, like login credentials for any other software, can be stolen and subsequently used to orchestrate an entire network attack.

What Are the Alternatives to VPNs?

Another illuminating finding from the report was that almost two-thirds (65%) of IT professionals say they are considering the adoption of VPN alternatives.

It's not wholly surprising, though, considering the prevalence of well-known exploits and the fact they can often reduce network speeds due to connection rerouting through different servers.

Zero-Trust Network Access (ZTNA) is an alternative that's becoming increasingly favored by businesses. According to the report, 80% of companies are in the process of adopting it.

Are VPNs Done for?

Not so soon. A good, reliable business VPN, despite the increased threat, is still good to have as part of your security infrastructure. Make sure employees are using a password manager, however (especially for their VPN login information) so that the risk of credential compromise is mitigated.

Source: https://tech.co/news/

Our CEO Is A Published Author

Stay one step ahead of cyber criminals to protect your business, your customers, and your money!

In Jason's first published book, he talks about why cybercrime today cannot be ignored and why your network and data are cyber criminals' #1 target!

Learn all the ways to protect yourself and your data. Contact us today for your copy of *Inside The Hacker Mind.*

Annual Halloween Costume Contest

Preferred IT Group held our annual Halloween costume contest again last month! There were some great costumes this year! The winner this year is Trevor Curry as a 50's Greaser.
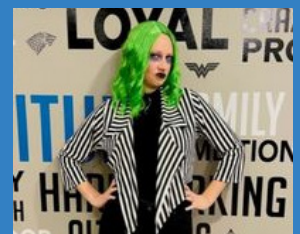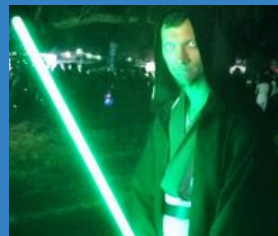
Socktober Success!

Our Socktober had a great turn out this year!

We were able to collect 1,121 pairs of socks, 4 hats, and 2 pairs of gloves! All of our donations went to the Fort Wayne Community Schools clothing bank.

Thank you so much to all of our clients who participated this year! We really appreciate you helping us to do our part for the community! You ROCK!

FUN FACT!

Apple's OS is more difficult to crack than Android system.

preferred IT group

CONTACT US

Fort Wayne
260.440.7377

Warsaw
574.306.4288

Columbia City
260.213.4266

Indianapolis
317.426.8180

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.