Malicious Azure Application PERFECTDATA SOFTWARE and Microsoft 365 Business Email Compromise - Syne's Cyber Corner

By syne0

Published: 2023-07-10 · Archived: 2026-04-02 10:36:27 UTC

Edit 04/13/25: The newest version of the software behind this application has changed. Now, the application's name within a tenant will be Mail_Backup. The app id is now 2ef68ccc-8a4d-42ff-ae88-2d7bb89ad139. Most of the information contained in this article is still accurate. Please view this post for up-to-date IOCs and permissions for this app.

If you have found your way to this page, you likely discovered a suspicious application consent within your Azure AD tenant for an app called PERFECTDATA SOFTWARE. Concerned, you googled the application (and perhaps even its Application ID ff8d92dc-3d82-41d6-bcbd-b9174d163620) looking for information. As of the time of writing, two other results on Google involve this software and BEC. If you haven't, I encourage you to read this darktrace.com article which goes further in-depth into a Microsoft 365 business email compromise (BEC). Unfortunately, Darktrace was unable to conclusively determine the purpose of the application consent. Luckily I have been able to find the application and examine its behavior.

The TL;DR

First, if you are seeing this application in your tenant and it's not approved, I have some bad news. This application is used to take a backup of the entire mailbox from the cloud and export it to PST. Assume that everything within the mailbox is lost, and any useful information will be used for future fraud or sold on the dark net. Oh, and if it was an administrative user compromised? It could potentially be every mailbox within the organization.

I'm sorry if I just ruined your day.

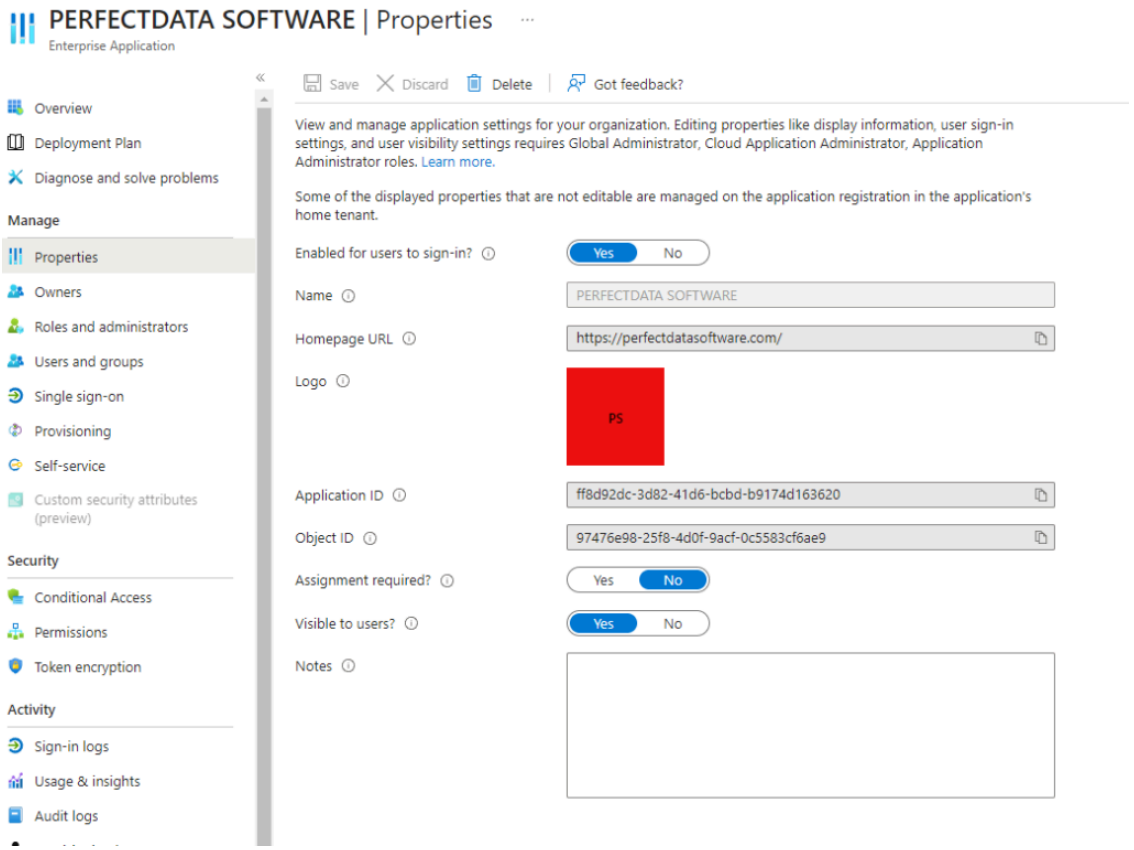
Applications Within Azure

An application can integrate with Microsoft 365 and Azure to do many things. The majority of applications that integrate with Azure do so for OAuth purposes so that you can sign into them with your Microsoft 365 credentials. Other applications integrate with Azure to provide you with a service, such as adding appointments created in a third-party app to your Microsoft 365 calendar. For those applications to access your Microsoft 365 account and its data, it must be granted the necessary permissions.

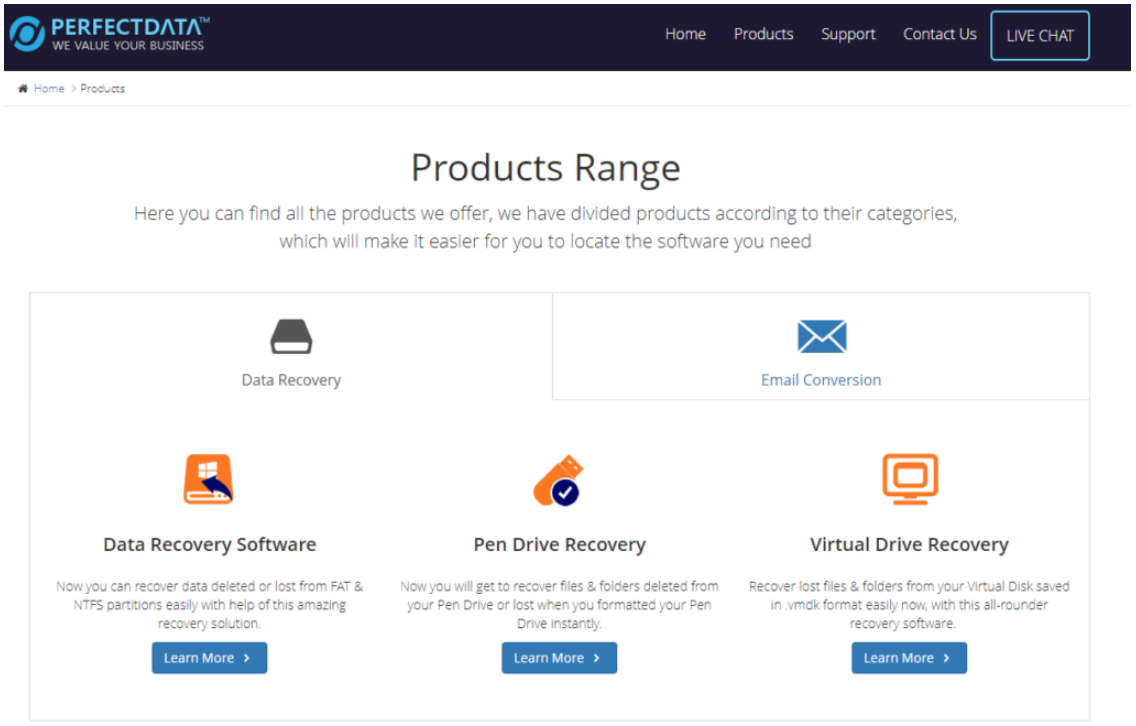
Perfectdata Software is an application that integrates with Microsoft 365/Azure to provide a service, as detailed below.

The Hunt

To begin, I will show you how I went from seeing this application within a tenant to learning what it does.

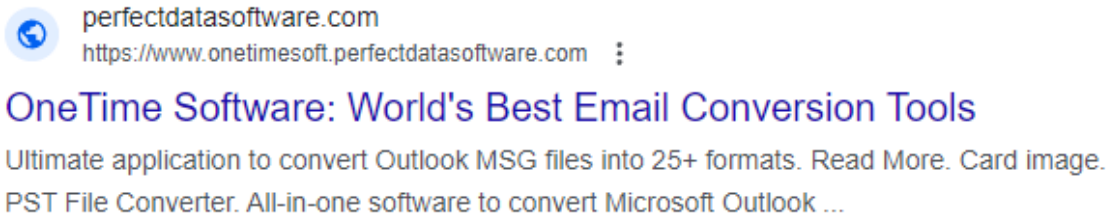


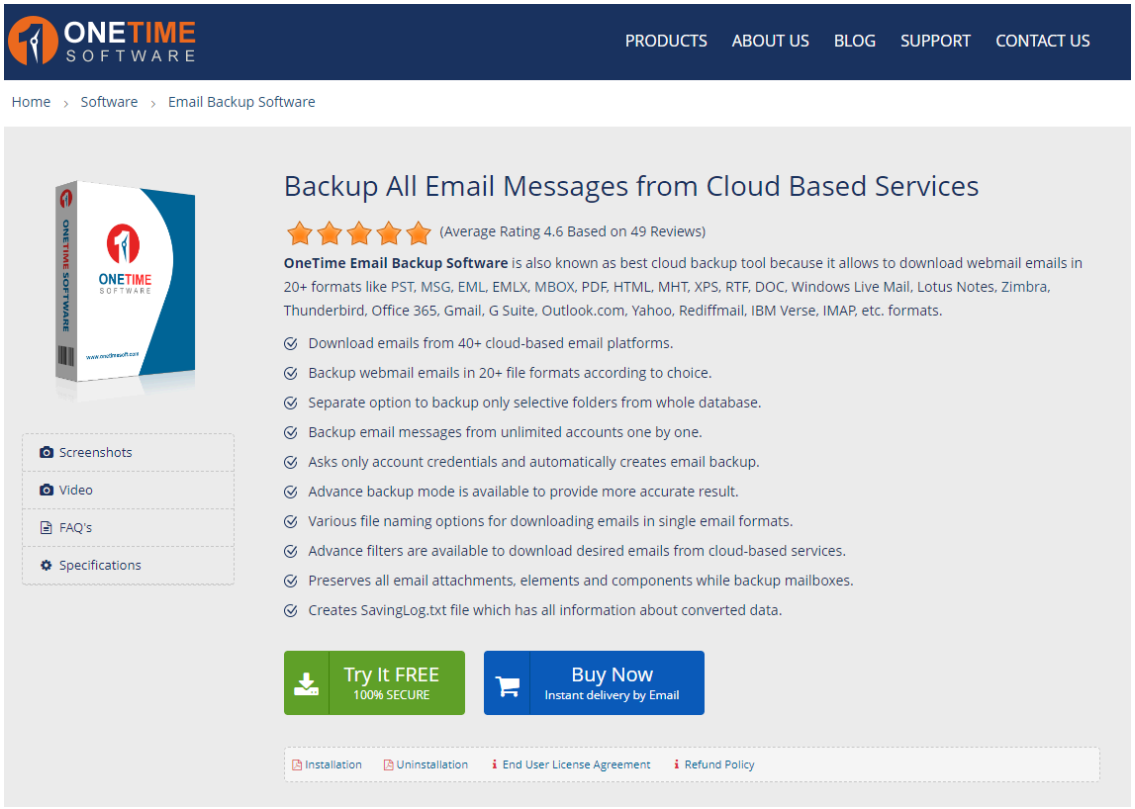
This is what you will see when viewing the application. Now, going to the website listed as the homepage URL takes you to a company that does data recovery and email conversion.



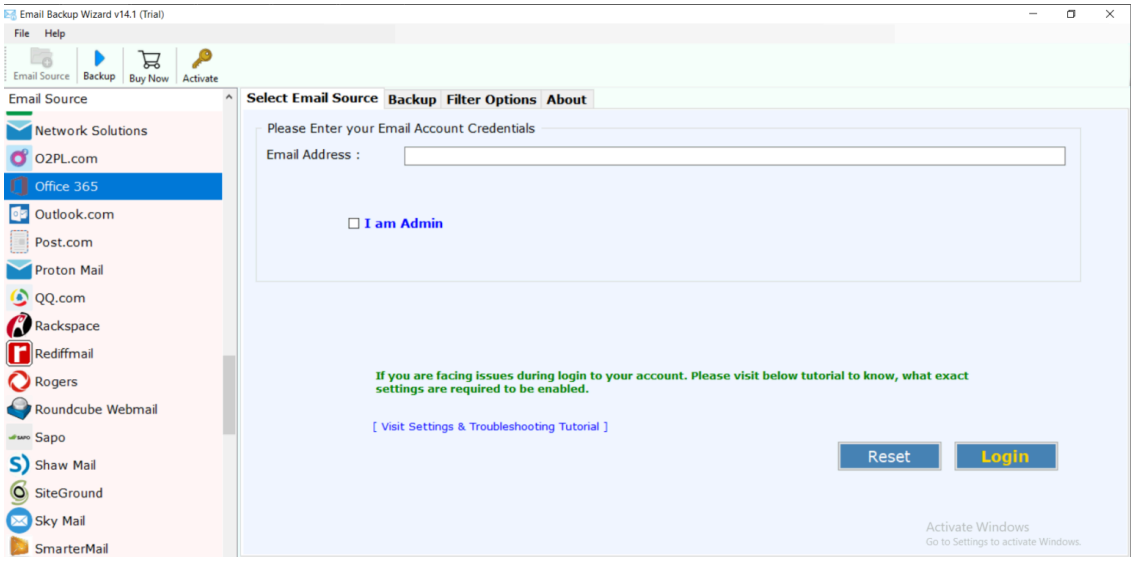
Hmm… not quite what I'm looking for.

Next, I decided to use one of my favorite OSINT tools- Google. I searched for site:perfectdatasoftware[.]com and oh boy, I got a lot of results. I'll eventually do a deep dive into this company, but to keep on track I found that perfectdatasoftware[.]com has many subdomains that redirect to other companies. This is the one that caught my eye, and it ended up being my lucky break.

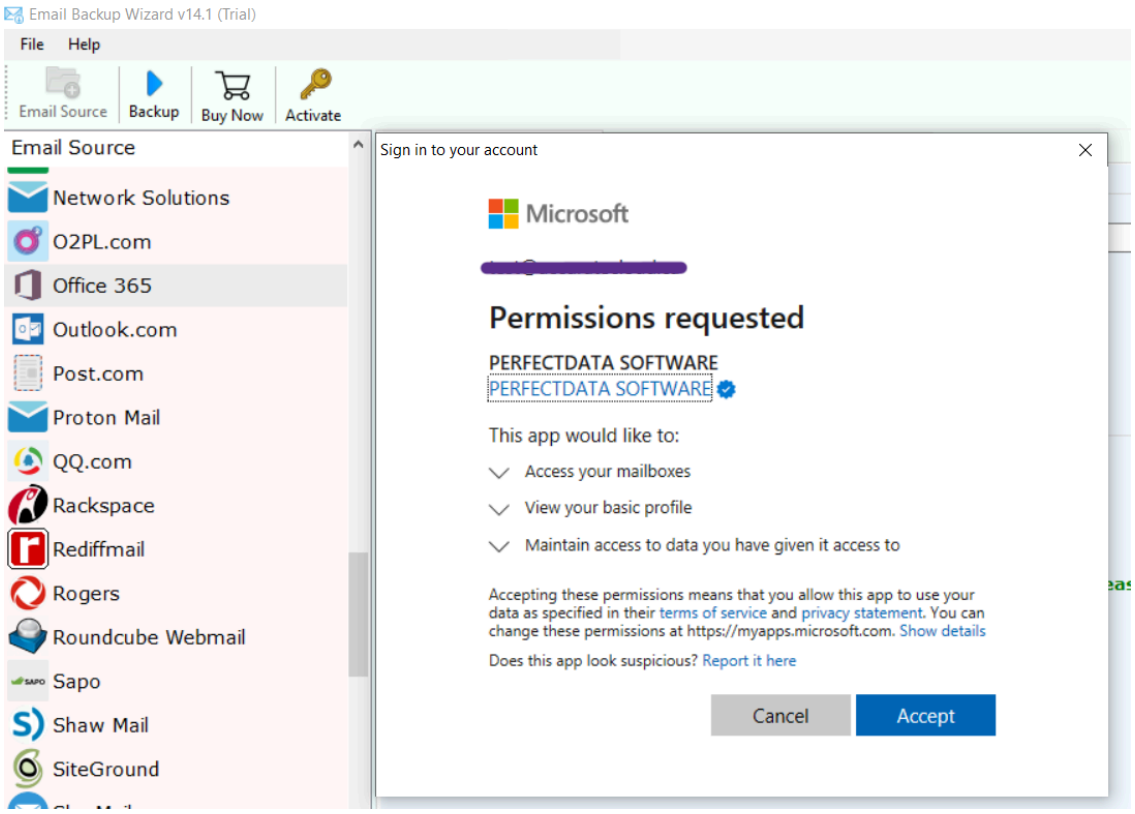




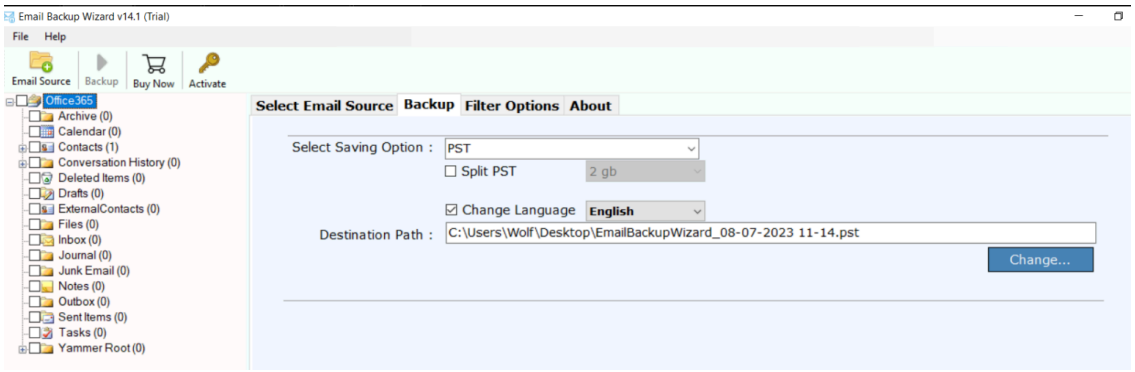
Let’s try this. I downloaded and installed the application, and upon opening it, was prompted to choose my cloud email provider and enter my credentials.



After entering my email, I am provided with the modern Microsoft 365 login. I enter my password, click sign in, and am presented with an application permission request.



Jackpot. After clicking accept, I am told to wait while it analyses my account. Finally, I am shown my Microsoft 365 folder, and the option to export it to PST. Since it's a PST, it grabs calendar events and contacts on top of emails and attachments.



And just like that, I can exfiltrate the mailbox offsite.

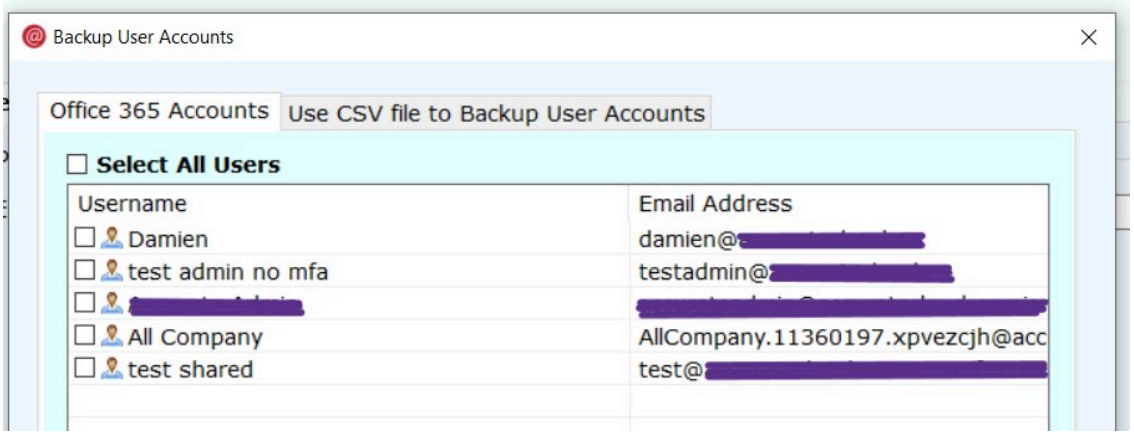
After testing, I was able to confirm that the application ID inside my test tenant matched the application ID I had seen in the BECs utilizing this application.

A Deeper Dive

As I have shown, when you see this application within your Microsoft 365 environment you should assume that the entire contents of the mailbox have been exfiltrated. Quite the privacy breach, no? Now, there's still some good news. My testing has shown me that this tool cannot be used to back up mailboxes that the user has

delegated access to. Some tools do that (so you should run access reports on delegated mailboxes that the compromised user has access to) but this is not one of them

Now, remember what I said about administrative users? Well, this tool will allow an administrative account to back up as many mailboxes as a person wants.



The provided documentation says that MFA must be disabled, the account must have application impersonation rights, and it needs delegate access to all mailboxes it wants to back up. I was able to get an admin account with MFA to back up mailboxes, as well as an administrative account that only had application impersonation rights.

If your tenant has access to the MailItemsAccessed record for the account in question, you may see that record with the service principal ID of the application. This isn't always the case, and since that record is less than helpful you should always assume all the email has been stolen.

What Now?

What you do now depends on your experience, the data involved, the scope of the issue, and any legal or compliance requirements/legislation that you must comply with.

First, do not delete this application from your tenant. You can go to the application within Azure, go to it's permissions, and click review permissions. If you designate the application as malicious, Microsoft will provide some handy PowerShell scripts for dealing with the application. It's important to disable the application but leave it in the tenant, as that will prevent anyone from being able to use it in the future.

If you believe that an administrative account was compromised, it's important to search through audit logs for any activity. Microsoft offers some guidance on dealing with an email compromise, which includes limited details about administrative account compromises. I personally use either the HAWK forensics tool or my own PowerShell module Osprey when investigating BEC, and it gathers helpful information about the tenant as part of it's initial tenant investigation. Unfortunately, those two options might not be enough. If you are a SMB dealing with this problem, then you should consider contracting third-party forensics.

You should also understand your requirements around compliance legislation. In Canada, any suspected privacy breach needs to be reported to the Privacy Commissioner. If there is a risk of harm related to any stolen personal

data, those affected must be notified of the breach. Other countries have similar legislation, but it's up to C-suite and Legal to determine next steps for those matters.

Finally, this is your sign to make some security improvements to your tenant. Azure AD/Entra ID Premium P1 or P2 are great, so choose licensing that includes one of those. You should also turn on administrator consent requests for risky applications. This prevents end users from granting an app access to more than it should have and allows you to review applications that have been added.

No matter the technical controls you put in place, alerting is very important. The most recent time I responded to a BEC including this application, was because I received an alert for it. There are plenty of tools for both SMB and Enterprise that have alerting for cloud email systems.

The Actual TL;DR

Having this application within your tenant is not a good sign. It allows a threat actor to exfiltrate the entire mailbox as a PST. If the threat actor has access to an administrative account, they can exfiltrate every single mailbox within the organization. This data includes all emails, attachments, calendar events, and contacts. The impact of this activity depends on the scope, what data was in the mailbox, and your compliance requirements. Limiting end user consent to applications can help prevent malicious application consents from affecting your tenant in the future.

Need Help?

If you read this article and have now come to the conclusion that you are experiencing an email compromise, it's normal to feel scared or uncertain, especially if you've never dealt with something as serious as this before. I have provided a guide for investigating an email compromise, so give it a look if you need. I can also be reached via LinkedIn, Email, or Discord to answer questions.

Unrelated Final Notes

If you like what I do and found this post helpful, please consider buying me a coffee on Ko-fi so I can continue to do more things like this.

This is the first blog entry/article I have written, so if you have any feedback I would appreciate it. I will update this article whenever I discover new information.

Thank you for reading my post!
