To the Editor May 4, 2020

Think you are Safe in the Cloud?

You are not Safe in the Cloud! How can Microsoft Azure, MS OneDrive, and Google AWS protect your systems and data, if they cannot protect their own? What follows is a summary and de-geekification of the information in the enclosed hyperlinks in an attempt to make it more understandable for the non-geek readers.

Cloud Identity is promoted as a great thing these days. You can sign up to lots of services using your social identity from Facebook, Google, or from Microsoft. You do not have to invent new passwords (or reuse passwords used elsewhere), and you get easy Single Sign On. This is sold as having more advantages than drawbacks for users, with little awareness of some of the dangers.

Think two factor authentication will protect you in the cloud? Think again. Even if an organization requires multi-factor authentication at sign-in, recall that a malware login process can take place on Microsoft's own Web site. In fact many of these malicious actors host their evil doing directly on Microsoft Azure sites. That means having two-factor enabled for an account would do nothing to prevent a malicious app that has already been approved by the user from accessing their emails or files. They use malicious a Microsoft Office 365 App to gain access to a victim's account without requiring them to give up their credentials to the attackers.

This is a long and fairly complex technical read, but if you are a business using cloud services, you better have your tech guys read this.

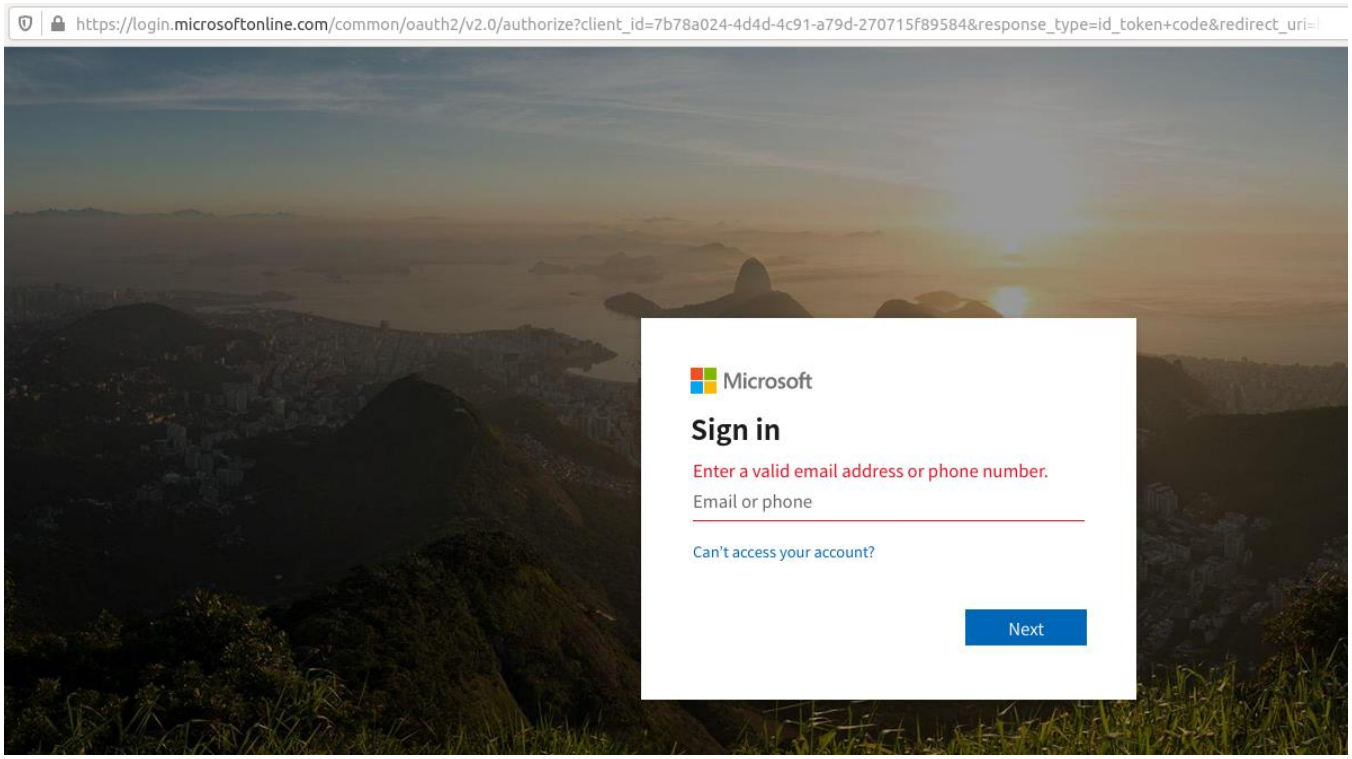
Late last year saw the re-emergence of a nasty phishing tactic that allows the attacker to gain full access to a user's data stored in the cloud without actually stealing the account password. The phishing lure starts with a link that leads to the real login page for a cloud email and/or file storage service. Anyone who takes the bait will inadvertently forward a digital token to the attackers that gives them indefinite access to the victim's email, files and contacts — even after the victim has changed their password.

Let us define what phishing is.

> *Phishing is using social engineering techniques to deceive computer and Internet users. These users are often lured into this by communications or prompts purporting to be from trusted parties.*

While the most recent phishing attacks target corporate users of Microsoft's Office 365 service, the same approach can be leveraged to attack users of many other cloud providers. In 2017 a similar technique was used to plunder accounts at Google's Gmail service.

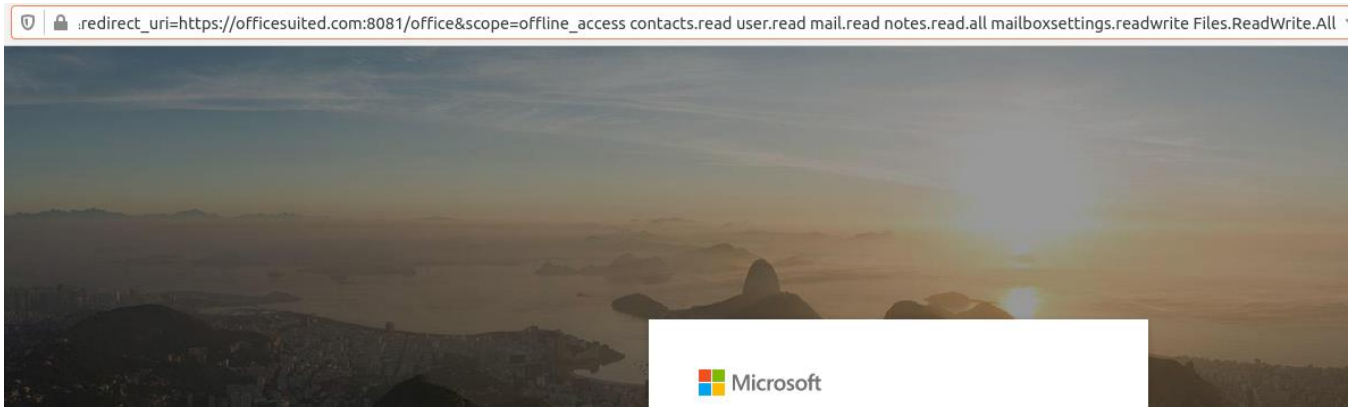
Security experts have identified a malicious link which took people who clicked to an official Office 365 login page— **login.microsoftonline.com** someplace else. Anyone suspicious about the link would have seen nothing immediately amiss in their browser's address bar, and could easily verify that the link indeed took them to Microsoft's real login page. See browser address bar below.



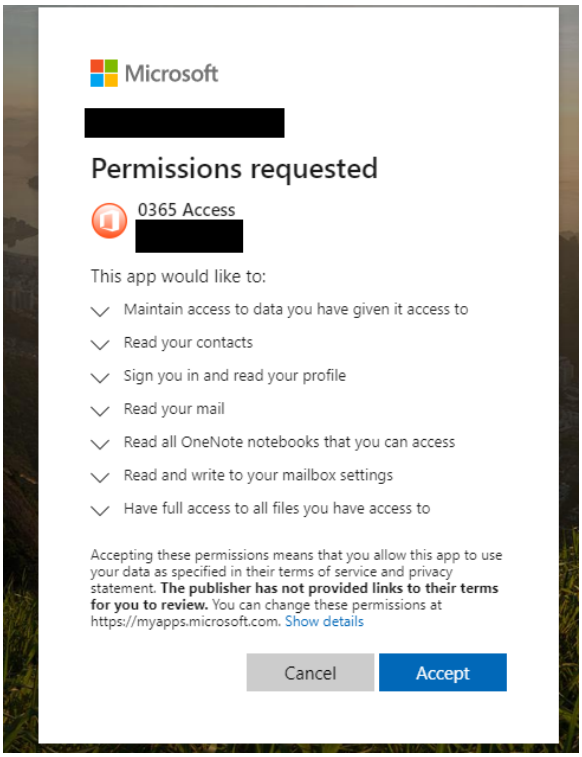
This phishing link asks users to log in at Microsoft's real Office 365 portal (login.microsoftonline.com).

Only by copying and pasting the link or by scrolling far to the right in the URL bar could you detect that something isn't quite right:

Notice this section of the URL (obscured off-page and visible only by scrolling to the right quite a bit) attempts to grant a malicious app hosted at officesuited.com full access to read the victim's email and files stored at Microsoft's Office 365 service.



As we can see from the URL in the image directly above, the link tells Microsoft to forward the authorization token produced by a successful login to the domain **officesuited[.]com**. From there, the user will be presented with a prompt that says an app is requesting permissions to read your email, contacts, OneNote notebooks, access your files, read/write to your mailbox settings, sign you in, read your profile, and maintain access to that data.



The app that generated this request was created using information stolen from a legitimate organization. The domain hosting the malicious app pictured above — **officemtr[.]com** — is hosted at the same Internet address as officesuited[.]com and likely signed using the same legitimate company's credentials.

These attackers are exploiting a feature of Outlook known as "add-ins," which are applications built by third-party developers that can be installed either from a file or URL from the Office store. By default, any user can apply add-ins to their outlook application as Microsoft allows Office 365 add-ins and apps to be installed via side loading without going through the Office Store, and thereby avoiding any review process.

This attack method is more like malware than traditional phishing, which tries to trick someone into giving their password to the scammers. Instead of handing off credentials to someone, they are allowing an outside application to start interacting with their Office 365 environment directly. How could the user somehow understand that there is a malicious third-party involved in this transaction, when the site *is* legitimate, and at that point their guard is down?

The scary part about this attack is that once a user grants the malicious app permissions to read their files and emails, the attackers can maintain access to the account even after the user changes his password. Only system administrators responsible for managing user accounts could see that the app had been approved.

Once given permission to access the user's email and files, the app will retain that access until one of two things happen: Microsoft discovers and disables the malicious app, or an administrator on the victim user's domain removes the program from the user's account.

Expecting swift action from Microsoft might not be ideal: From my testing, Microsoft appears to have disabled the malicious app being served from officesuited[.]com sometime around Dec. 19 — roughly one week after it went live.

In a statement provided to KrebsOnSecurity, Microsoft Senior Director Jeff Jones said the company continues to monitor for potential new variations of this malicious activity and will take action to disable applications as they are identified.

"The technique described relies on a sophisticated phishing campaign that invites users to permit a malicious Azure Active Directory Application," Jones said. "We've notified impacted customers and worked with them to help remediate their environments."

Microsoft's instructions for detecting and removing illicit consent grants in Office 365 are here. Microsoft says administrators can enable a setting that blocks users from installing third-party apps into Office 365, but

it calls this a “drastic step” that “isn’t strongly recommended as it severely impairs your users’ ability to be productive with third-party applications.”

PhishLabs’ Tyler said he disagrees with Microsoft here, and encourages Office 365 administrators to block users from installing apps altogether — or at the very least restrict them to apps from the official Microsoft store.

Apart from that, he said, it’s important for Office 365 administrators to periodically look for suspicious apps installed on their Office 365 environment.

“If an organization were to fall prey to this, your traditional methods of eradicating things involve activating two-factor authentication, clearing the user’s sessions, and so on, but that won’t do anything here,” he said. “It’s important that response teams know about this tactic so they can look for problems. If you can’t or don’t want to do that, at least make sure you have security logging turned on so it’s generating an alert when people are introducing new software into your infrastructure.”

Don’t take my word for any of this, here are some comments from the web:

“I personally have seen Microsoft account phishing sites hosted on Azure.”

“App permissions page? The unfortunate thing is that people don’t read those and just blindly hit “Accept”.

“Over 90% of security incidents are caused by either people doing something they shouldn’t do, or someone not doing something they should do. Humans aren’t perfect, shocking, I know, but it’s true. The brightest people in the world, yes even “security experts,” can fall for a scam if you catch them at the right time.”

“The root cause is the many years that Microsoft has taught users to click by rote: “Next > Next > Next ….”, “OK > OK > OK….” , “I Agree > I Agree > I Agree…”, “Accept > Accept > Accept…”

“The “Cloud” is getting darker by the day. I wonder if this is huge rigged three card Monty scam or a well-choreographed multinational confidence game. I am dubious MS is actually putting their customer’s security over their corporate profits. Data harvesting seems to be a big winner for certain big players these days.”

“First, while the most recent versions of this stealthy phish targeted corporate users of Microsoft’s Office 365 service, the same approach could be leveraged to ensnare users of many other cloud providers. Second, this attack is not exactly new: In 2017, for instance, phishers used a similar technique to plunder accounts at Google’s Gmail service.”

“The link contains standard OAuth functionality: – it directs Microsoft to give access to the users’ resources to a consumer (in this case, the attacker)– Microsoft correctly asks the users if they’re ok with this– The users reply “yes”, granting the attacker access”

“Really the only cleverness here is getting the user in a context where such a prompt is not unexpected, therefore multiplying the chances that the users will click “yes”.

“Seems like bullet hole in Microsoft’s cloud.”

We should all be concerned about this.

Sources:

https://krebsonsecurity.com/2020/01/tricky-phish-angles-for-persistence-not-passwords/ - more-50056
https://securityintheenterprise.blogspot.com/2019/11/microsoft-azuread-and-office365-not.html
https://info.phishlabs.com/blog/office-365-phishing-uses-malicious-app-persist-password-reset
https://duo.com/blog/gmail-oauth-phishing-goes-viral
https://krebsonsecurity.com/2020/01/phishing-for-apples-bobbing-for-links/