Microsoft warns of phishing campaigns targeting Outlook Web App and Office 365 users

Microsoft security experts issue an important warning about an ongoing large-scale phishing, targeting Outlook Web App (OWA) services and Office 365.

According to preliminary statistics from the end of December 2020 to now, more than 400,000 login information of OWA and Office 365 users worldwide has been stolen. In addition, there are signs that this malicious campaign is continuing to scale and sophistication to abuse new legitimate services, with the ultimate goal of bypassing secure email gateways (Secure Email Gateways - SEGs).

The recently documented attacks are in fact part of a series of phishing campaigns collectively known as the "Compact" Campaign, which has been going on since early 2020.

" *Scammers continue to succeed in using compromised accounts on email marketing services, then using these accounts to send malicious emails from legitimate IP domains and ranges",* Microsoft security experts said. *"They take advantage of legitimate configuration settings to ensure they can send malicious emails, bypass phishing email detection solutions* ."

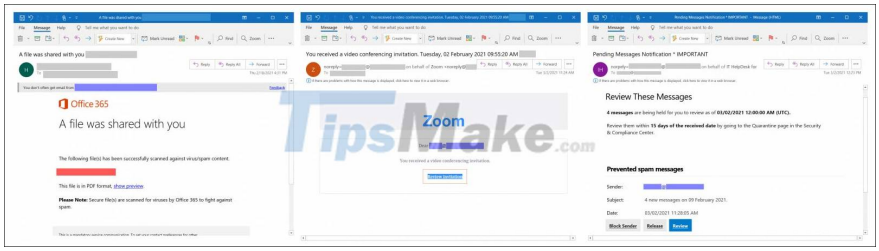
Outdid the SEGs

The attackers behind this phishing campaign stole more than 400,000 Office 365 and Outlook Web Access credentials since last December. Their phishing emails are disguised as announcements from video conferencing services, various security solutions, as well as business support solutions for added legitimacy.

In addition, hackers also used the compromised accounts for the SendGrid and MailGun emailing services, taking advantage of secure email portals to legalize malicious activity, making them listed as worthy domains. trust. This allows a large amount of phishing emails to bypass the SEG security barrier and reach the target's inbox.

When victims click on links embedded in malicious emails, they are immediately redirected to phishing landing pages, designed to impersonate Microsoft login pages.

" *In December 2020, the malicious landing page in this campaign impersonated an Outlook Web App service to trick the target into entering their credentials. In January 2021, the fake landing page resumed its replacement. change, impersonate the Office 365 login website to steal the login information of users of this service* ', the report from WMC Global pointed out.



As observed by security experts, this fraud is showing signs of increasing, as scammers are also abusing both Amazon's Simple Email Service (SES) and cloud computing platform Appspot (used to develop and host web applications in Google-managed data centers) to send phishing emails and generate multiple impersonating URLs targeting each target.