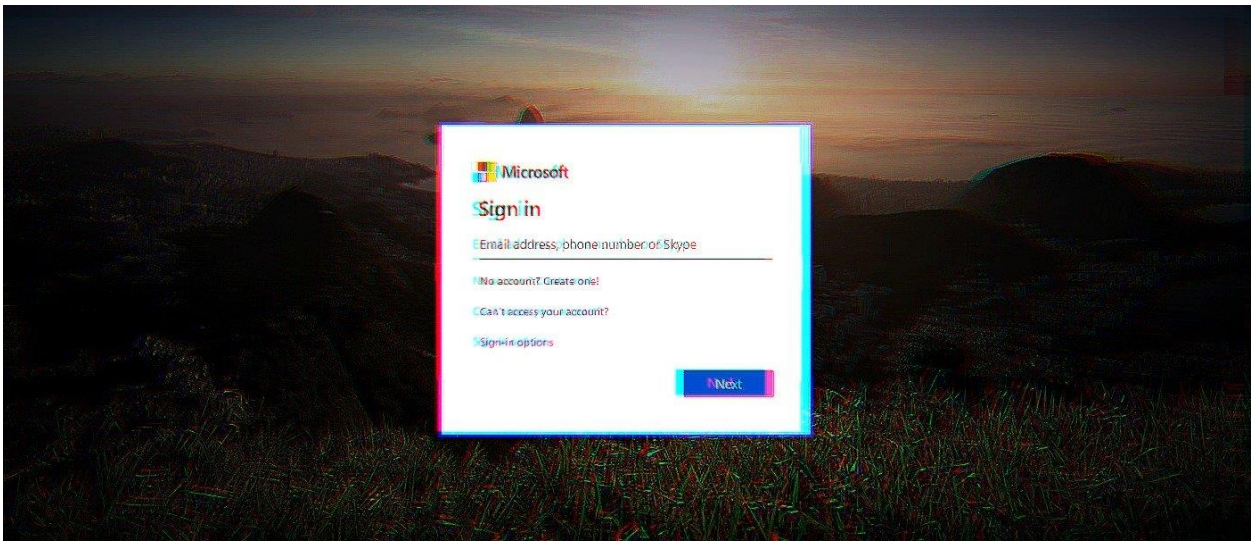
Office 365 phishing abuses Google Ads to bypass email filters



An Office 365 phishing campaign abused Google Ads to bypass secure email gateways (SEGs), redirecting employees of targeted organizations to phishing landing pages and stealing their Microsoft credentials.

The attackers behind these attacks took advantage of the fact that the domains used by Google's Ads platform are overlooked by SEGs, which allows them to deliver their phishing messages to their targets' inboxes bypassing email filters.

SEGs are designed to block spam and phishing attempts from reaching their users' mailboxes using filtering stacks that will scan all incoming emails for malicious content.

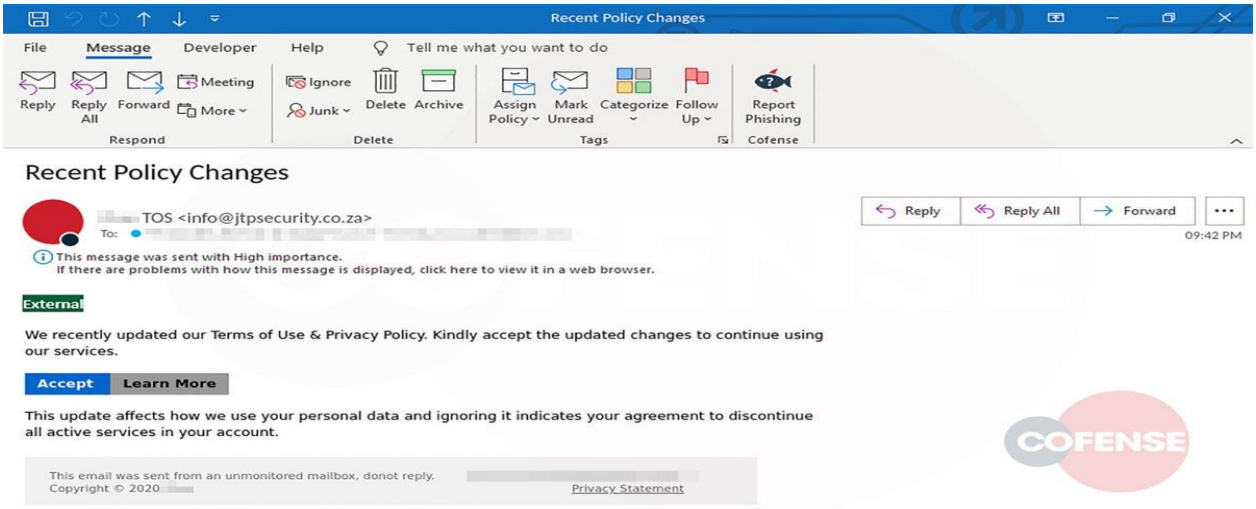
Targeted phishing campaign

The phishing emails were sent to employees of multiple organizations from compromised accounts as Cofense Phishing Defense Center (PDC) researchers who spotted this campaign found.

Potential victims are informed of recent policy changes and are asked to accept the changes to be able to continue using services.

The accept button embedded within the phishing emails, however, will redirect the victims to phishing landing pages with the help of a Google Ads redirect.

This hints at the fact that the attackers paid for a Google ad and then used the ad's URL to redirect targets to pages used to steal Office 365 credentials, thus making sure that the victims always receive their phishing messages.



The phishing pages used in this campaign are designed to mimic legitimate Microsoft pages, featuring a Microsoft logo and the targets' company logo.

Targets are first sent to a cloned Microsoft privacy policy page and then to the final phishing page that mimics the victims' company-branded Office 365 sign-in pages

Once they entered their credentials and hit the "Next" button, their account info was immediately sent to the phishers and they were sent to a new page displaying a "We've updated our terms." message.

As a final measure designed to hide the attack from the victims, the employees who fell victim to this phishing attack were sent to the Microsoft Services Agreement page.

Phishers have used a wide array of tactics to make sure that their phishing messages have a higher chance to circumvent their targets' email protection filters.

A recent example is a highly targeted Bank of America phishing campaign that sent emails with body contents free of links to malicious-looking domains, using SendGrid to successfully pass SPF, DKIM, and DMARC authentication checks.

Other phishers have bypassed security filters in the past by using QR codes and WeTransfer file-sharing notifications to make sure that their emails reached their targets' inboxes.

They were also seen abusing Google Docs, Google Drive, and Microsoft SharePoint as part of phishing campaigns capable of dodging SEGs to infect victims with malware or to steal their credentials and financial info.

References:

- https://www.bleepingcomputer.com/news/security/office-365-phishing-abuses-google-ads-to-bypass-email-filters/?&web_view=true
- https://malware-guide.com/blog/attackers-abuses-google-ads-with-a-new-campaign-to-bypass-email-filters
- https://cloudsek.com/threatintel/office-365-phishing-targets-google-ads-startups-suffer-data-breach-386m-records-leaks-and-more/