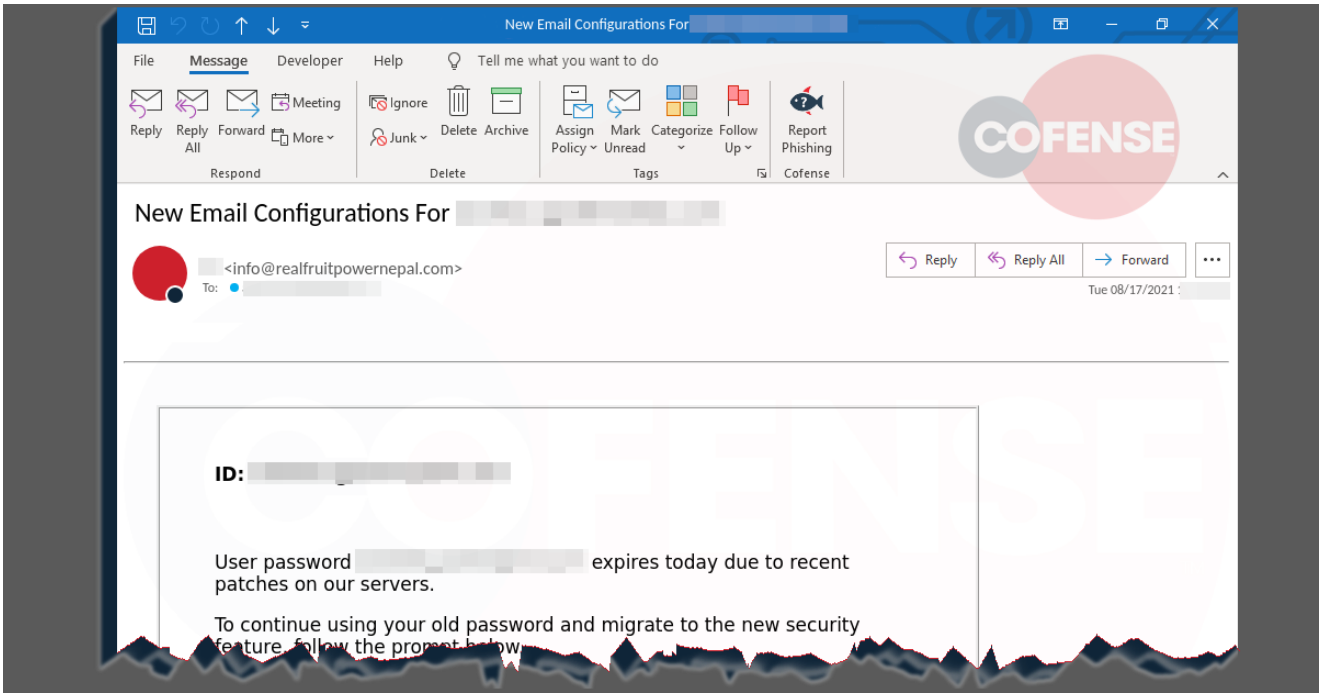
“Missed Voice Message,” the Latest Phishing Lure

cofense.com/blog/missed-voice-message-phish/

Cofense October 21, 2021



Phish Found in Environments Protected by SEGs

Microsoft

Ironport

By Adam Martin, Cofense Phishing Defense Center

Recently, the Phishing Defense Center (PDC) has observed a trend relative to a phishing tactic involving missed voicemail messages. As illustrated below in figure 1, the end user is notified about a missed voice message from a British Telecom landline. The link directs the recipient to a website that isn’t in any way associated with BT or any other legitimate telecom service.

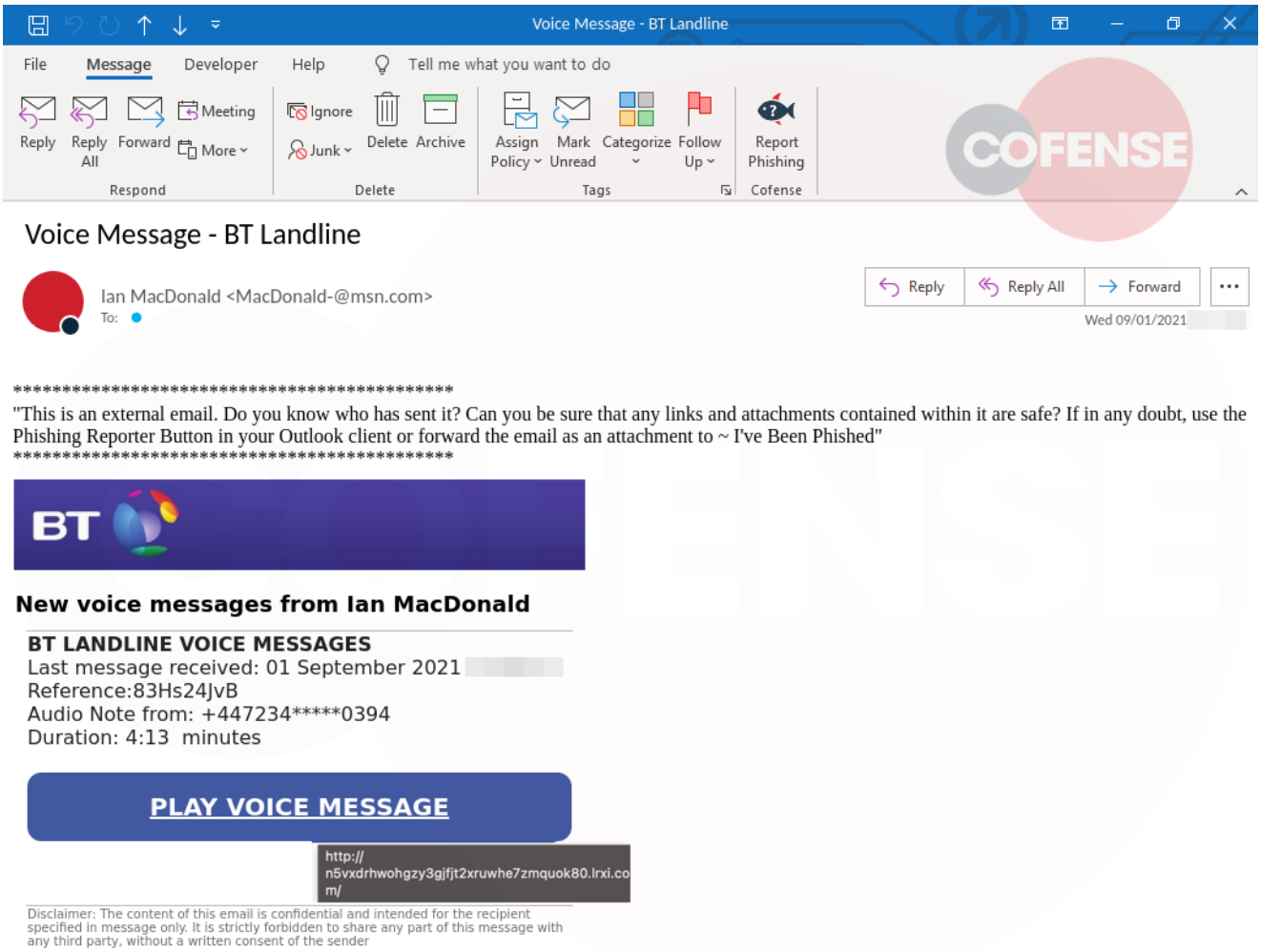


Figure 1: Initial Email

Once this malicious link is accessed, the recipient is directed to the landing page seen in figure 2. This page purports to be the BT sign-in page, spoofing the BT logo and reminding the recipient of their missed messages. One minor detail worth noting is that the number of voice messages pending has changed from one to three. This is likely due to the same mass phishing mail being sent out with the parameter of one voice message, and the pre-set HTML code in the phishing page being set to three. A slight oversight on the part of the threat actor, but the page remains convincing, nevertheless.

Once the recipient has entered their details, this information is exfiltrated to an external private address. As is observable from the URL bar of figure 2, the corresponding URL could hardly be more clearly not the BT sign-in page.

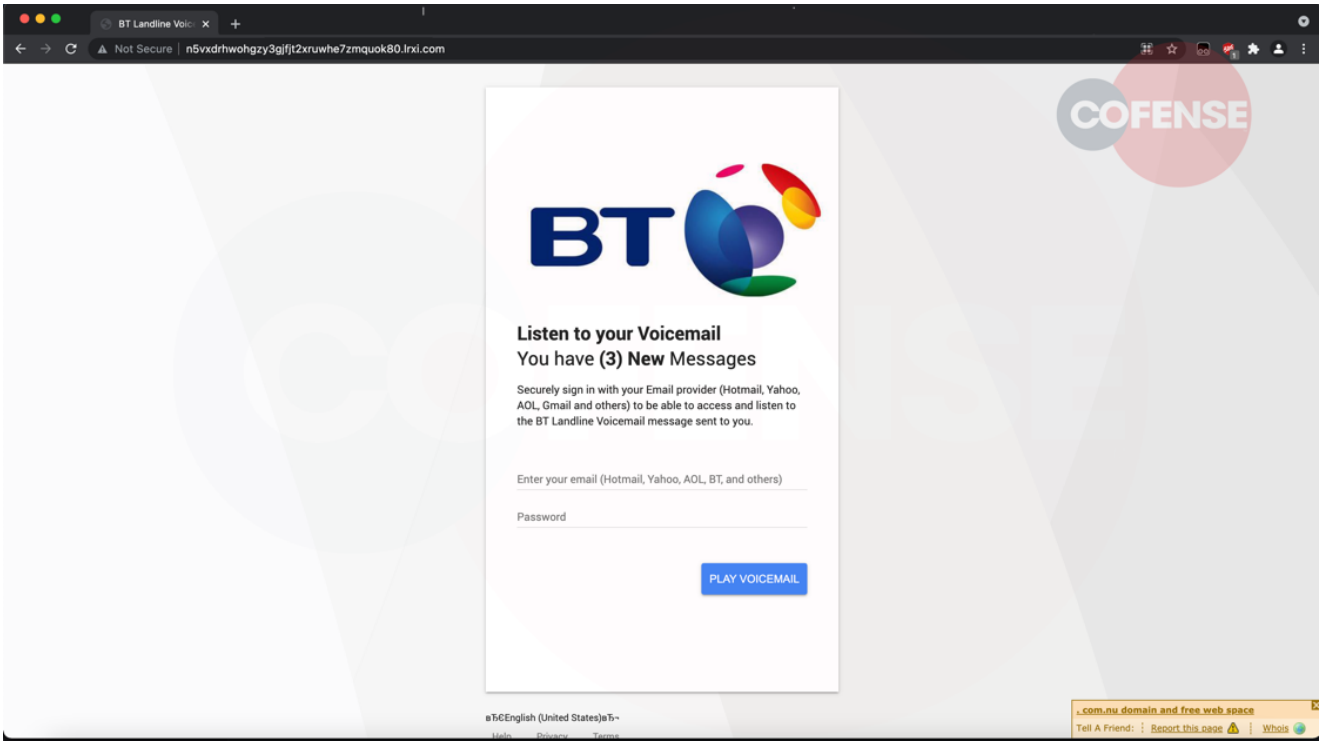


Figure 2: Landing Page

As with many phishing landing pages, regardless of the details entered, the page will redirect back to the target companies' home page. This event campaign is no different. Once credentials are entered and data stolen, the recipient is directed straight to the official BT help page. This is done to boost perceptions of "legitimacy."

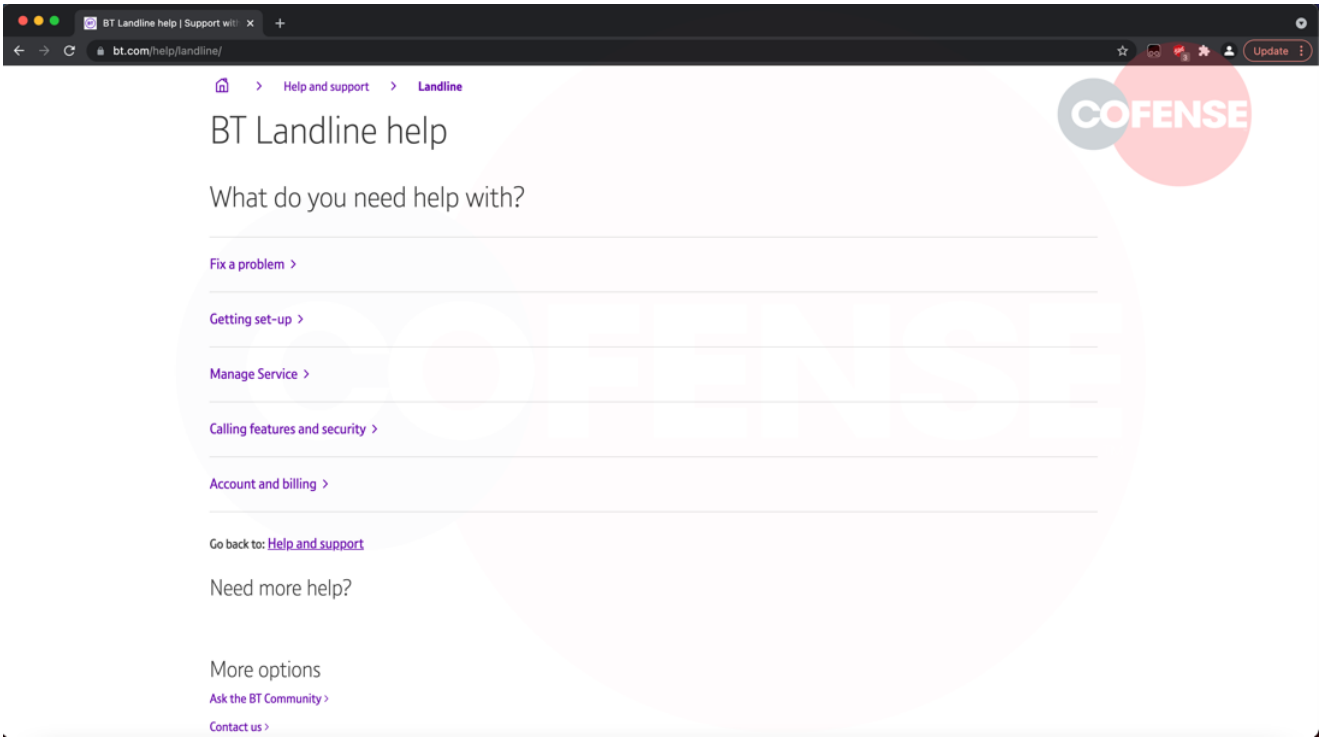


Figure 3: BT Homepage

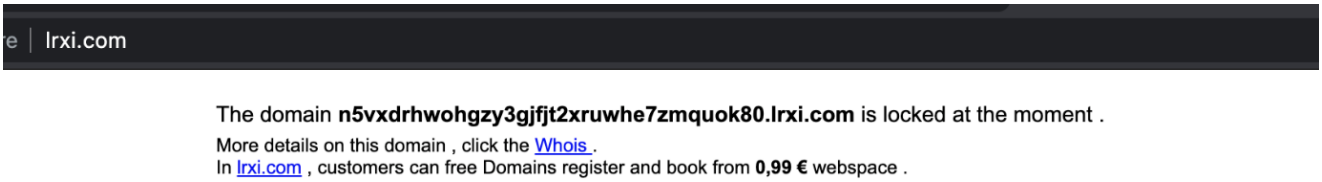


Figure 4: Landing Page as it stands

Missed voice messages as a phishing tactic continues to be a trend, leads to one conclusion: A high success rate. The landing page or provider will change depending on the targeted region but one thing remains certain. The tactic will continue in tandem with the threat actor success.

Cofense is here to help with our analysts and technology to enable users to quickly identify validated or newly observed threats. We have the necessary products to help your SOC team isolate threats to reduce risk and further leverage the IOCs to mitigate a potential incident. Contact us to learn more.

Indicators of Compromise

http://n5vxdrhwohgzy3gzy3gjft2xruwhe7zmquok80.lrxi.com	144.76.162[.]245

Don't miss out on any of our phishing updates! Subscribe to our blog.