"Missed Voice Message," the Latest Phishing Lure

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

Cofense

October 21, 2021

File <u>Message</u> Developer	Help Q Tell me wh	Email Configurations For hat you want to do	P (- 0	×
Reply Reply Forward 🛱 More ~ All Respond	∑ Junk ~ Delete Archive Delete	Assign Mark Categorize Policy ~ Unread ~ Tags	Follow Report Up ~ Phishing		COF	INSE	
New Email Configura		Tays	.a. corense				
<info@realfruitpo< p=""></info@realfruitpo<>	wernepal.com>			← Reply	≪ Reply All	\rightarrow Forward	
To: •						Tue 08/17/2021 :	
ID:		expires today	due to recent				
ID: User password patches on our		expires today	due to recent				

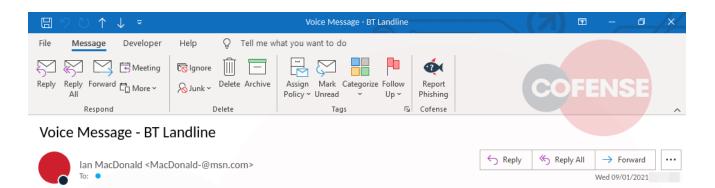
Phish Found in Environments Protected by SEGs

<u>Microsoft</u>

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.



"This is an external email. Do you know who has sent it? Can you be sure that any links and attachments contained within it are safe? If in any doubt, use the Phishing Reporter Button in your Outlook client or forward the email as an attachment to ~ I've Been Phished"

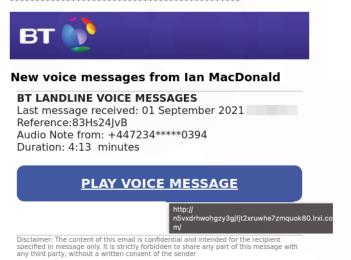


Figure 1: Initial Email

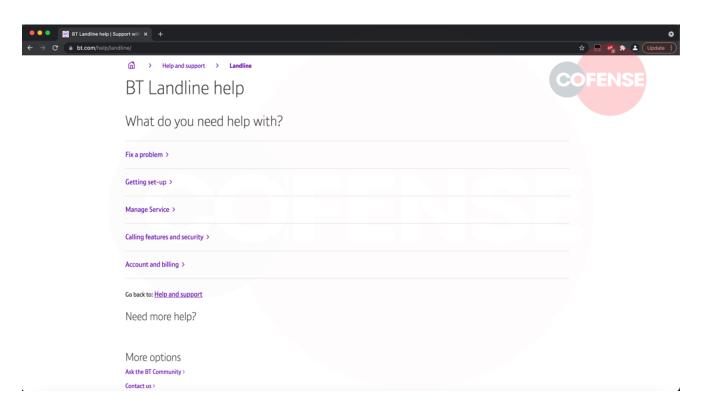
Once this malicious link is accessed, the recipient is directed to the landing page seen in figure 2. This page purports to be the BT sign-in page, spoofing the BT logo and reminding the recipient of their missed messages. One minor detail worth noting is that the number of voice messages pending has 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.

BT Landline Volci X +		0
← → C ▲ Not Secure n5vxdrhwohgzy3gjfjt2xruwhe7zmquok80.lrxi.com		# 🖈 💀 🗛 🛊 💷 E
		COFENSE
	BT	
	Liston to your Veicemeil	
	Listen to your Voicemail You have (3) New Messages	
	Securely sign in with your Email provider (Hotmail, Yahoo, AOL, Gmail and others) to be able to access and listen to	
	the BT Landline Voicemail message sent to you.	
	Enter your email (Hotmail, Yahoo, AOL, BT, and others)	
	Password	
	PLAY VOICEMAIL	
	sTreEnglish (United States)sTr Melon Privacy Terms	. com.nu domain and free web space Image: Compare the space Tell A Friend: Report this page: A I Whois (Compare the space)

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."



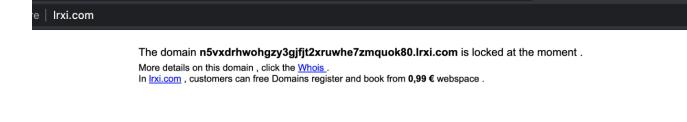


Figure 4: Landing Page as it stands

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

All third-party trademarks referenced by Cofense whether in logo form, name form or product form, or otherwise, remain the property of their respective holders, and use of these trademarks in no way indicates any relationship between Cofense and the holders of the trademarks. Any observations contained in this blog regarding circumvention of end point protections are based on observations at a point in time based on a specific set of system configurations. Subsequent updates or different configurations may be effective at stopping these or similar threats.

The Cofense® and PhishMe® names and logos, as well as any other Cofense product or service names or logos displayed on this blog are registered trademarks or trademarks of Cofense Inc.

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