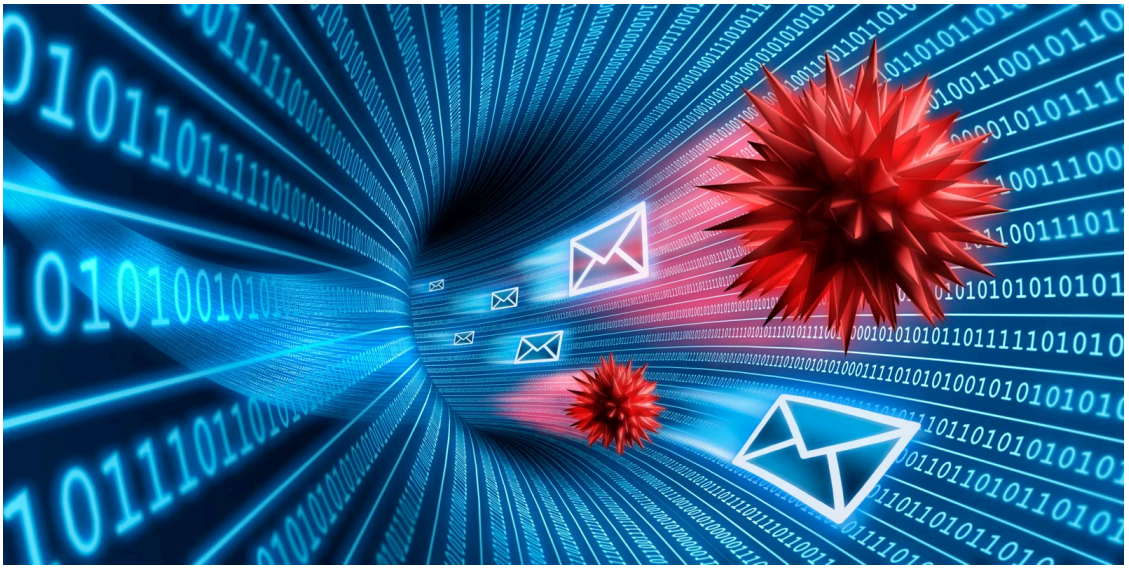
Dridex Omicron phishing taunts with funeral helpline number

By Lawrence Abrams

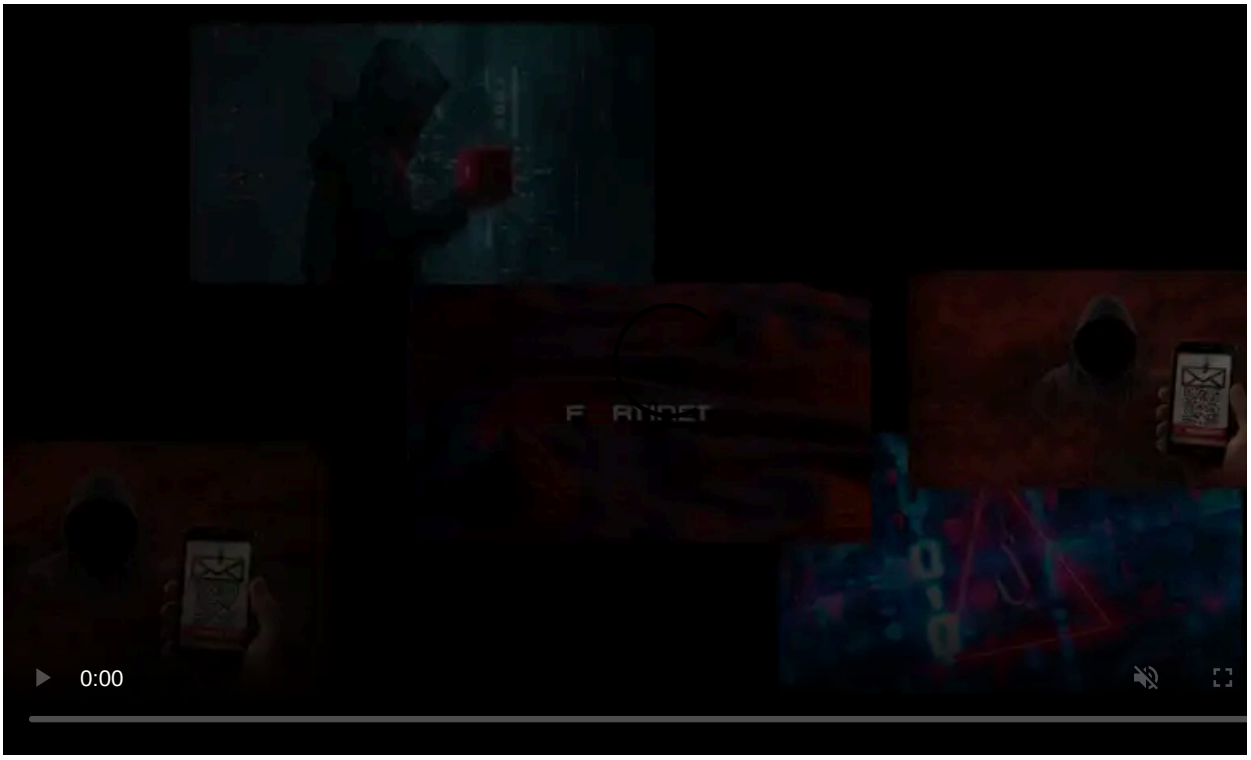
Published: 2021-12-24 · Archived: 2026-04-05 23:01:02 UTC



A malware distributor for the Dridex banking malware has been toying with victims and researchers over the last few weeks. The latest example is a phishing campaign that taunts victims with a COVID-19 funeral assistance helpline number.

Dridex is banking malware distributed through phishing emails containing malicious Word or Excel attachments. When these attachments are opened, and macros are enabled, the malware will be downloaded and installed on the victim's device.

Once installed, Dridex will attempt to steal online banking credentials, spread to other machines, and potentially provide remote network access for ransomware attacks.


0:00

COVID-19 Omicron variant used as a lure

Over the past few weeks, one of the Dridex phishing email distributors is having fun toying with victims and researchers.

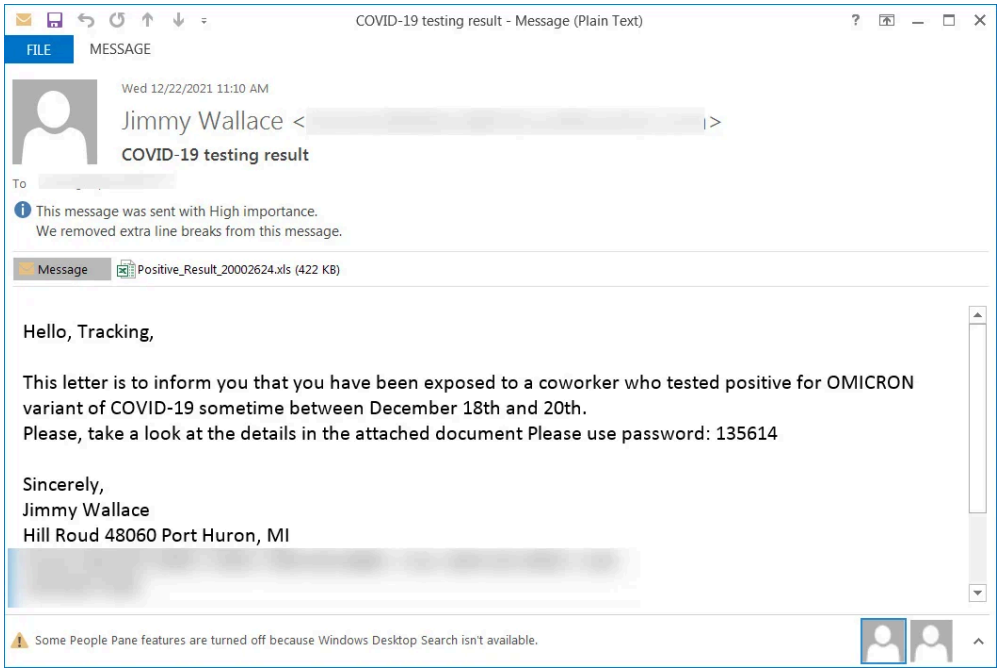
This was first seen when the threat actor began trolling security researchers by using their names combined with racist comments as malware file names and email addresses.

Earlier this week, the threat actor spammed fake employee termination letters that displayed an alert stating, "Merry X-Mas Dear Employees!", after infecting their device.

In a new phishing campaign discovered by MalwareHunterTeam and 604Kuzushi, this same threat actor took it to the next level by spamming emails with a subject of "COVID-19 testing result" that states the recipient was exposed to a coworker who tested positive to the Omicron COVID-19 variant.

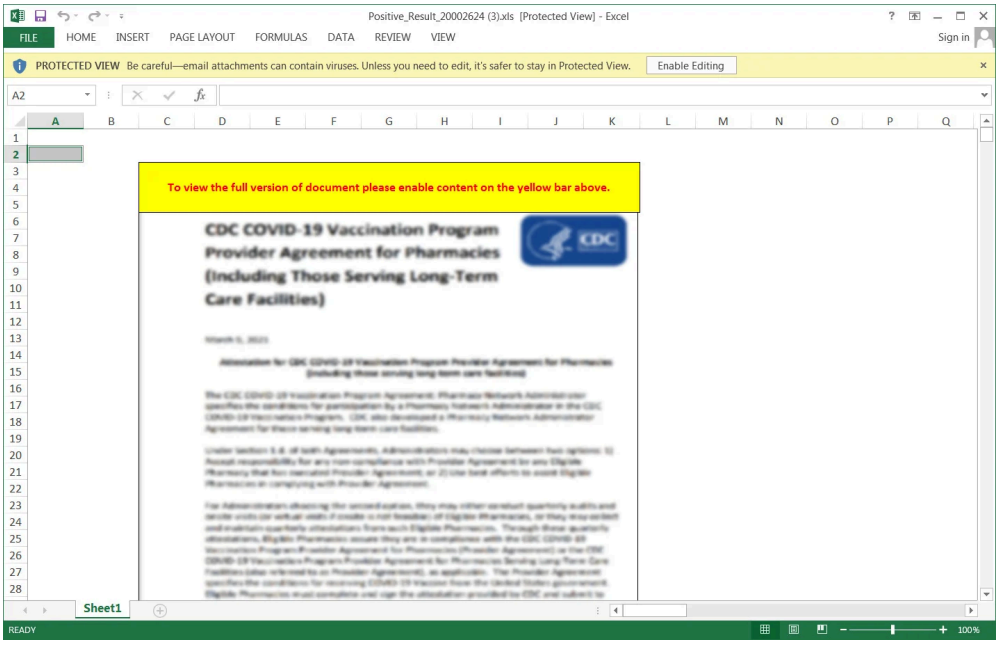
"This letter is to inform you that you have been exposed to a coworker who tested positive for OMICRON variant of COVID-19 sometime between December 18th and 20th," reads the new phishing email shown below.

"Please take a look at the details in the attached document."



Dridex phishing email stating you were exposed to Omicron COVID-19 variant

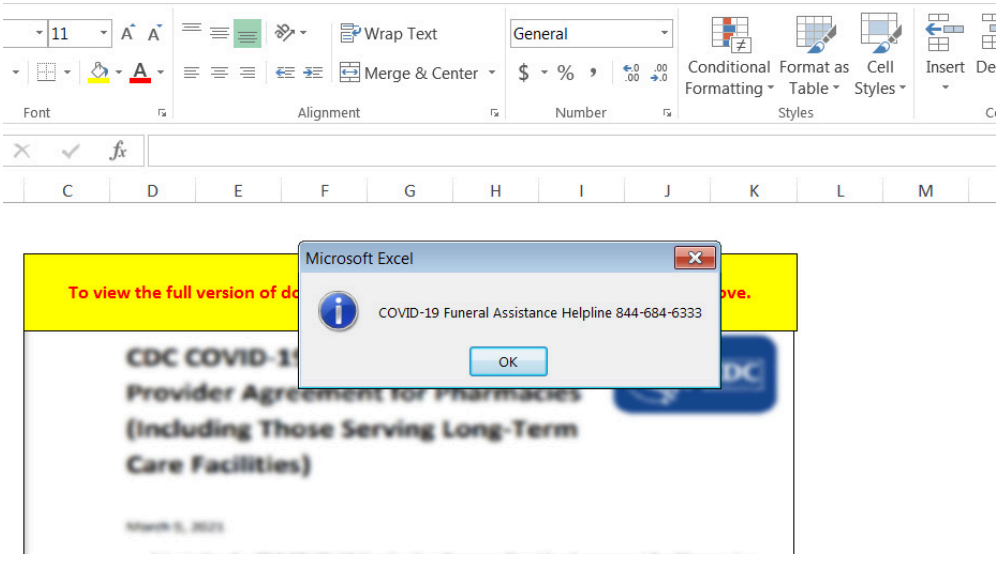
The email includes a password-protected Excel attachment and the password needed to open the document. Once the password is entered, the recipient is shown a blurred COVID-19 document and is prompted to 'Enable Content' to view it.



Blurred document lure to convince users to enable macros

Source: BleepingComputer

To add insult to injury, after macros are enabled, and the device becomes infected, the threat actor taunts their victims by displaying an alert containing the phone number for the "COVID-19 Funeral Assistance Helpline."



A bad joke showing the COVID-19 Funeral Assistance Helpline number

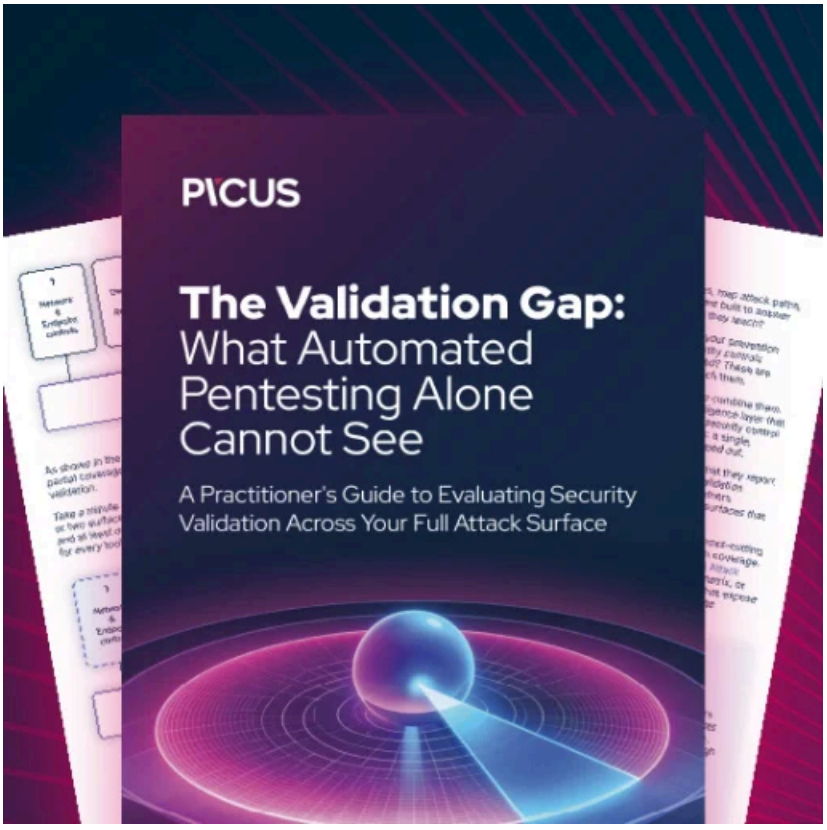
Source: BleepingComputer

With the COVID-19 variant being highly contagious and rapidly spreading worldwide, phishing emails about the Omicron variant are becoming popular and are likely highly effective in distributing malware.

This is especially true if the phishing campaign pretends to be from a company's human resources department and targets employees from the same company.

As Dridex phishing campaigns are currently using password-protected attachments, enterprises need to train their employees to spot and avoid these types of attacks.

As always, if you receive unexpected emails or one that contains unusual attachments, always reach out to your network admin or other people in the workplace to determine if the email is legitimate.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/dridex-omicron-phishing-taunts-with-funeral-helpline-number/