Dridex malware trolls employees with fake job termination emails

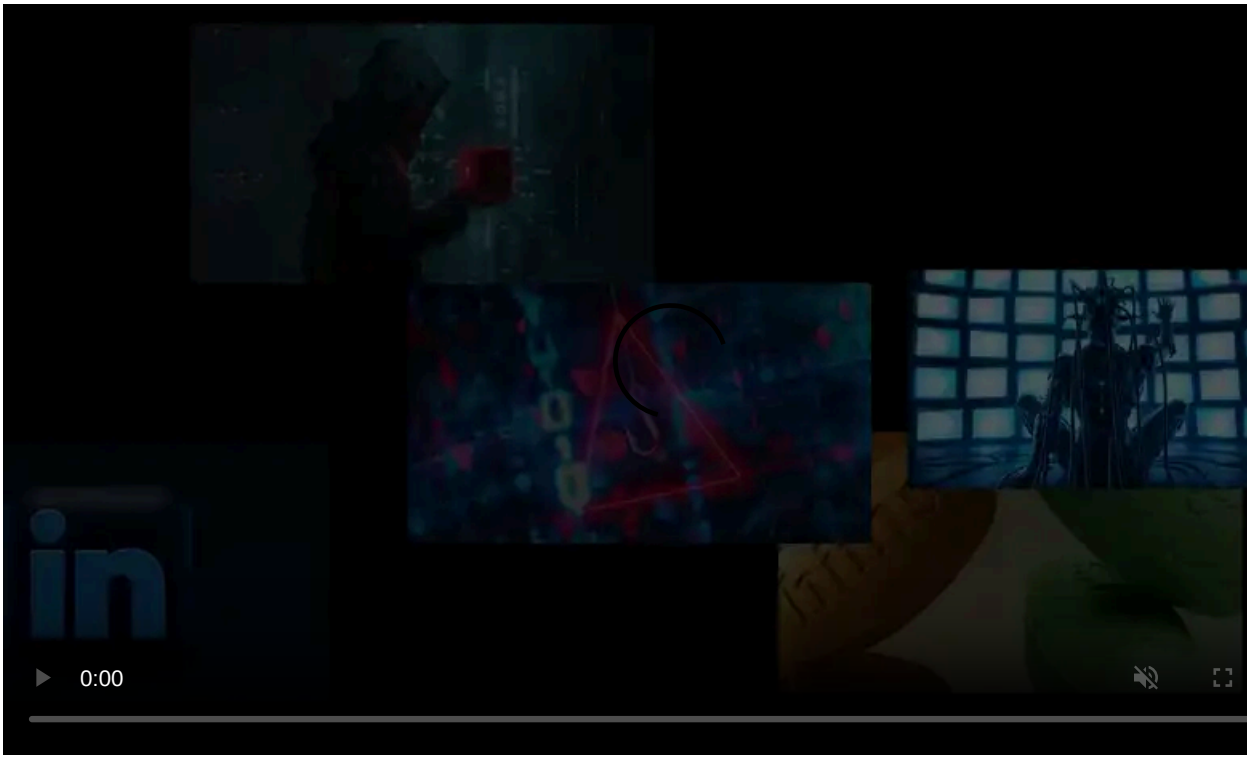
By Lawrence Abrams

Published: 2021-12-22 · Archived: 2026-04-05 18:13:32 UTC

A new Dridex malware phishing campaign is using fake employee termination emails as a lure to open a malicious Excel document, which then trolls the victim with a season's greeting message.

Dridex is a banking malware spread through malicious emails that was initially developed to steal online banking credentials. Over time, the developers evolved the malware to use different modules that provide additional malicious behavior, such as installing other malware payloads, providing remote access to threat actors, or spreading to other devices on the network.

This malware was created by a hacking group known as Evil Corp, which is behind various ransomware operations, such as BitPaymer, DoppelPaymer, WastedLocker variants, and Grief. Due to this, Dridex infections are known to lead to ransomware attacks on compromised networks.


0:00

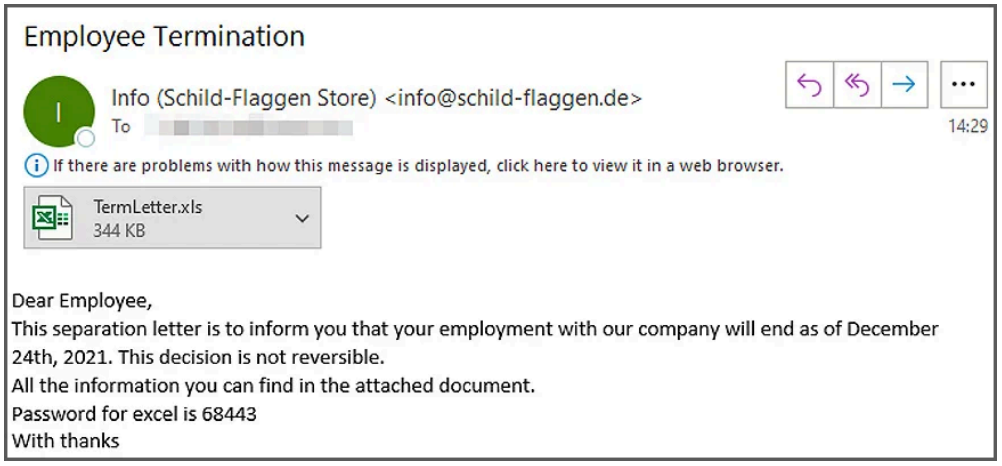
Dridex affiliate trolls researchers, victims

A Dridex affiliate has been conducting numerous malicious email campaigns over the past few weeks where they troll researchers with email addresses and filenames composed of racist and antisemitic words.

A security researcher known as TheAnalyst discovered that Dridex is again trolling people, but this time it's the victims who are being sent fake employee termination emails.

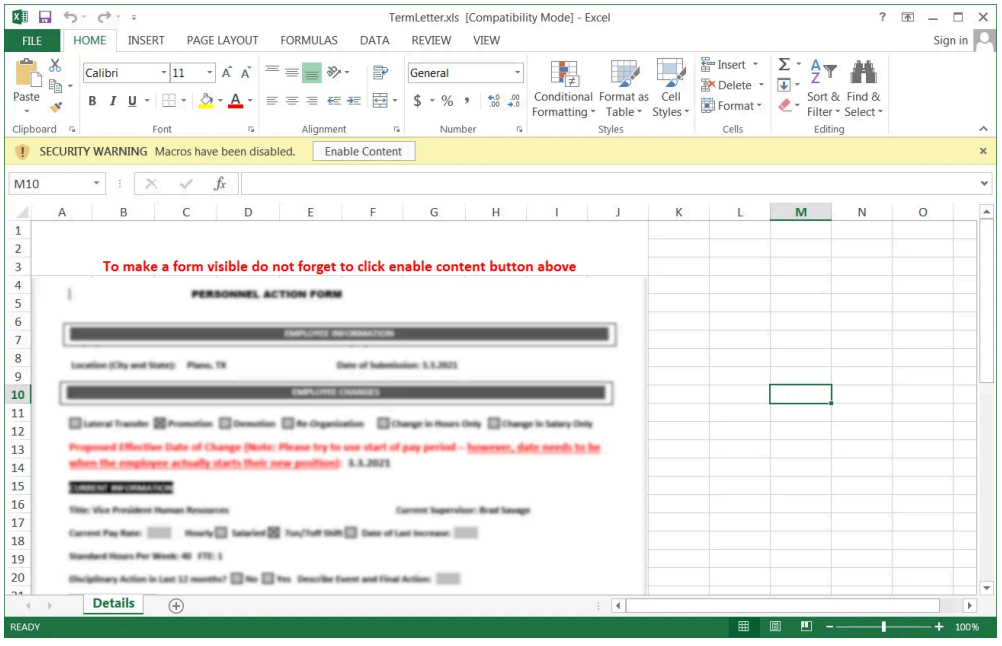
These emails use the subject of "Employee Termination" and tell the recipient that their employment is ending on December 24th, 2021, and that "this decision is not reversible."

The emails include an attached Excel password-protected spreadsheet named 'TermLetter.xls' that allegedly contains information on why they are being fired and the password required to open the document.



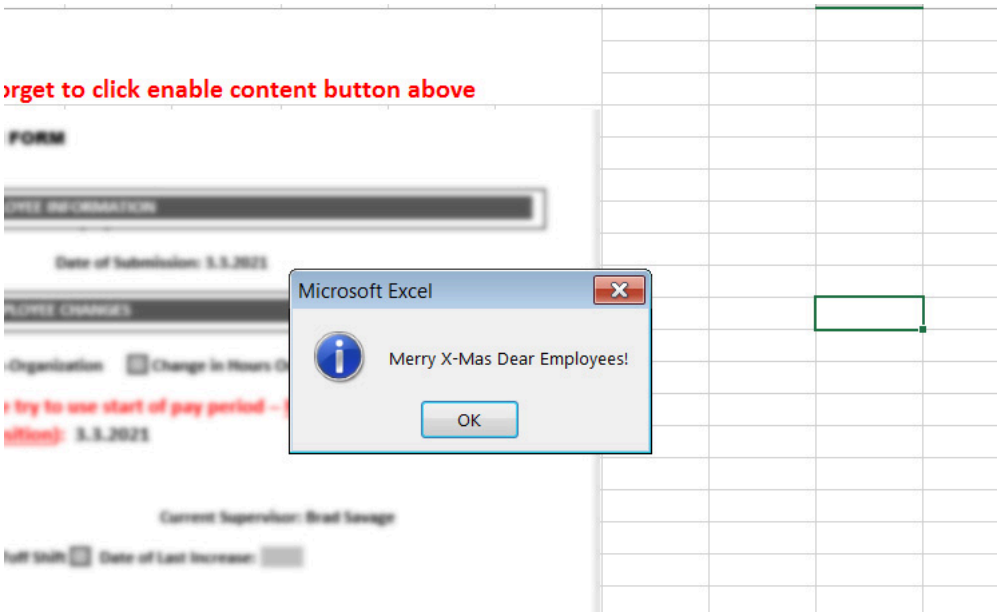
Dridex Employee Termination phishing email

When the recipient opens the Excel spreadsheet and enters the password, a blurred "Personnel Action Form" will be displayed, saying they must "Enable Content" to view it properly.



Malicious Excel attachment

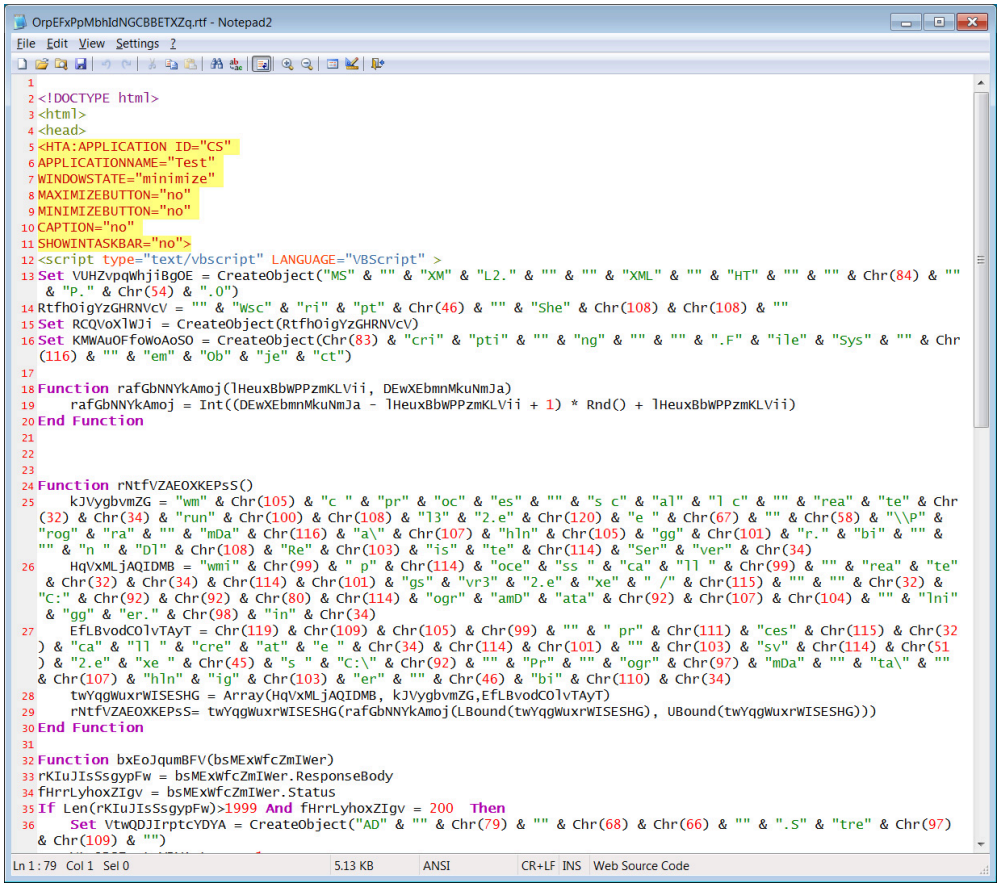
When the victim Enables Content, a popup will be displayed trolling the victim with an alert stating, "Merry X-Mas Dear Employees!"



Dridex distributor trolling victims

However, unbeknownst to the victim, malicious macros have been executed that create and launch a malicious HTA file saved to the C:\ProgramData folder.

This random-named HTA file pretends to be an RTF file but contains malicious VBScript that downloads Dridex from Discord to infect the device, all while wishing the victim a Merry Christmas.



Malicious HTA file disguised as an RTF file

As a little extra "joke," the TheAnalyst told BleepingComputer that the Dridex file downloaded from Discord is named 'jesusismyfriend.bin.'

Once Dridex is launched, it will begin installing additional malware, stealing credentials, and performing other malicious behavior.

Therefore, if you receive an email stating you are fired right before Christmas, be sure to reach out to your human resources department or employer before opening the email.

As Dridex infections commonly lead to ransomware attacks, Windows admins need to stay on top of the latest malware distribution methods and train employees on how to spot them as well.

Source: https://www.bleepingcomputer.com/news/security/dridex-malware-trolls-employees-with-fake-job-termination-emails/