Watch Out: There's A 'Big' Black Lives Matter Scam About

Cybercriminals are trying to profit from the Black Lives Matter protests. (AP Photo/Rick Bowmer)

-Thomas Brewster, Forbes

Cybercriminals are continuing to show they have no class. After jumping on the COVID-19 pandemic to launch masses of scams, they're now looking to spread dangerous malware by luring Americans in with Black Lives Matter-related phishing attacks in the middle of the widespread protests supporting the black community.

In a phishing attack caught by cybersecurity outfit abuse.ch, spam emails are going out with the subject line: "Vote anonymous about 'Black Lives Matter.'" There's not much in the content of the email, just the statement: "Leave a review confidentially about Black Lives Matter... Claim in attached file."

It's hardly the most sophisticated attack, just about mysterious enough to catch out at least some folks interested in the movement. If any curious party clicks on the attached file it ends up installing a dangerous Microsoft Windows malware known as TrickBot.

"From what I see is that the spam campaign was pretty big, apparently hitting US mailboxes," a spokesperson from abuse.ch told *Forbes*. "Historically, TrickBot is an e-banking trojan.

However, these days TrickBot is heavily used by various threat actors to install additional malware on the victim's computer. In corporate networks, this usually leads to Ransomware such as Ryuk."

As *Forbes* previously reported, Ryuk is one of the most prevalent ransomwares used by cybercriminals as they try to lock up people's digital files and unlock them only in return for payment. It was once, mistakenly, linked to North Korea. Instead, it appears to be a highly successful cybercriminal operation that's made its owners many millions of dollars.

Practising good cyber hygiene should help protesters trying to stay safe online in these trying times. In this case, that means being suspicious of any emails asking you to click on attachments, especially if they're from unknown sources.