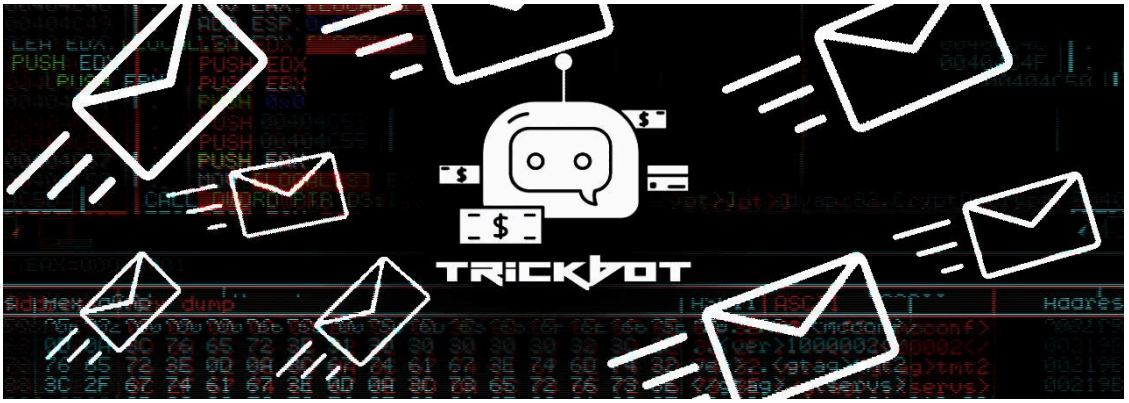
Fake Black Lives Matter voting campaign spreads Trickbot malware

By Lawrence Abrams

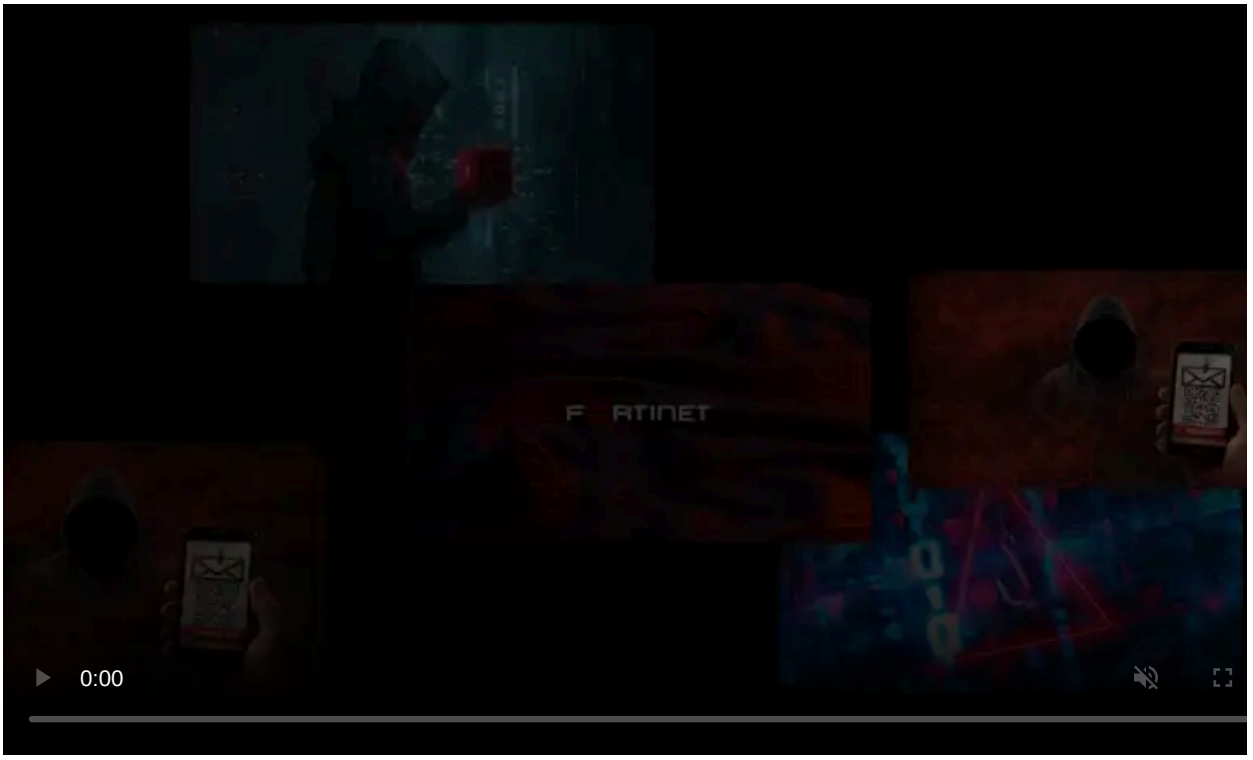
Published: 2020-06-10 · Archived: 2026-04-05 23:48:51 UTC

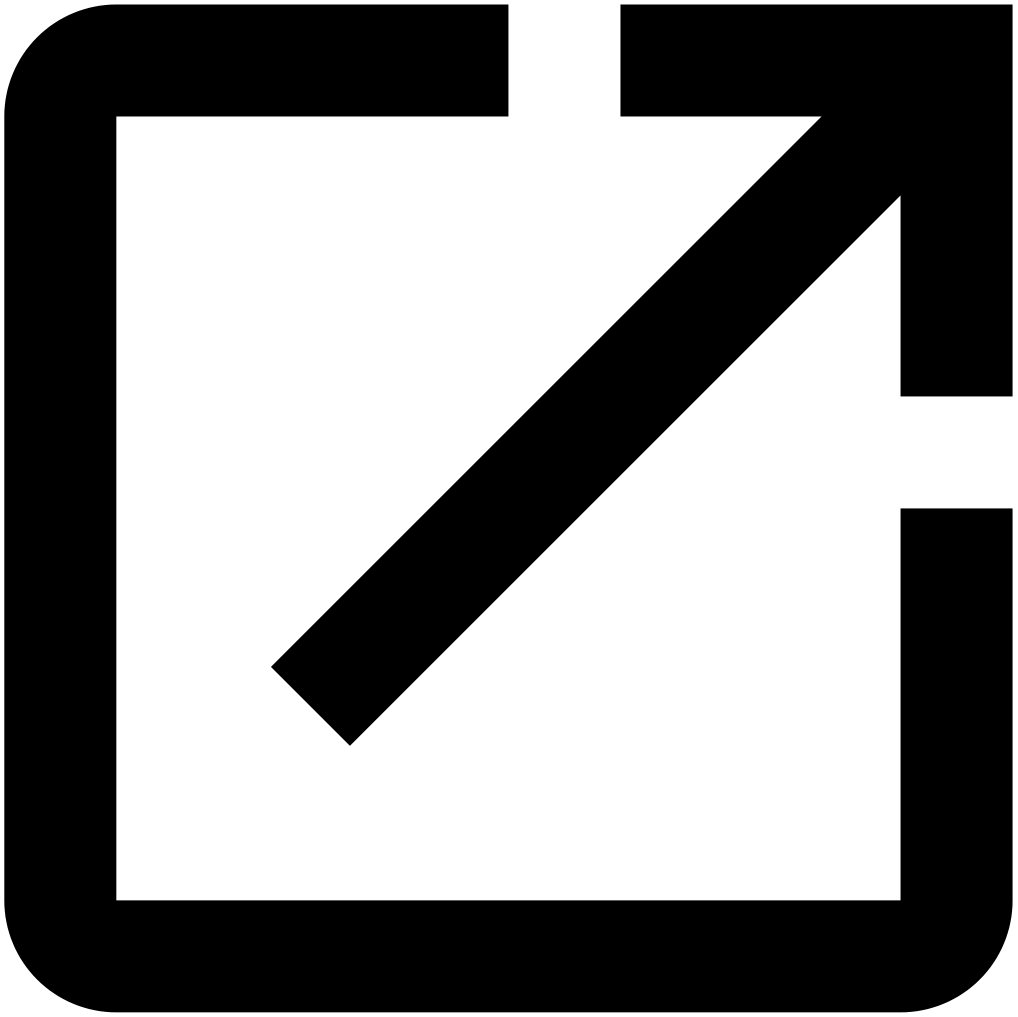


A phishing email campaign asking you to vote anonymously about Black Lives Matter is spreading the TrickBot information-stealing malware.

Started as a banking Trojan, the TrickBot has evolved to perform a variety of malicious behavior.

This behavior includes spreading laterally through a network, stealing saved credentials in browsers, stealing Active Directory Services databases, stealing cookies and OpenSSH keys, stealing RDP, VNC, and PuTTY Credentials, and more.


F RTINET
0:00



TrickBot also partners with ransomware operators, such as Ryuk, to give access to a compromised network to deploy ransomware.

Capitalizing on the Black Lives Matter movement

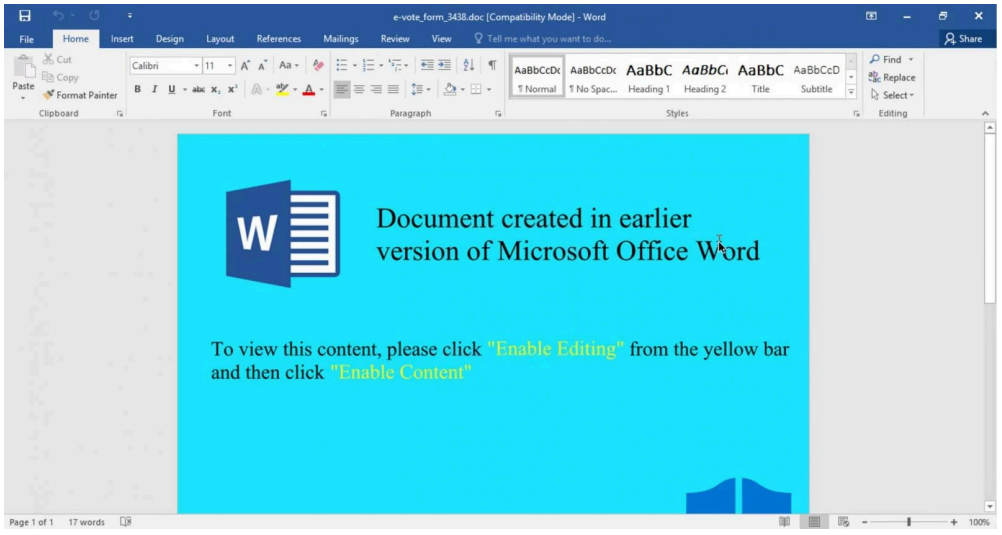
Threat actors commonly utilize current events as lures to trick people into opening their malicious emails.

Such is the case with a new campaign discovered by cybersecurity organization Abuse.ch that pretends to be from "Country administration," asking recipients to 'Vote anonymous about "Black Lives Matter".'

The email, shown below, states, "Leave a review confidentially about "Black Lives Matter" and then prompts recipients to fill out and return an attached document named 'e-vote_form_3438.doc.'

Phishing email

When a recipient opens the Word document, they will be greeted with a message stating that they need to click on the 'Enable Editing' and 'Enable Content' buttons to view the contents properly.



Malicious word doc

Once they click on these buttons, the Word document will run macros that download a malicious DLL to the computer and execute it.

This DLL is the TrickBot trojan that, when executed, will download further modules to the infected computer to steal files, passwords, security keys, spread laterally throughout the network, and allow other threat actors to install ransomware.

Due to this, a TrickBot trojan can be a devastating infection regardless of whether you are a corporate victim or a home user.

It is important to remember that malware developers and distributors commonly become more active during significant moments in history and political unrest.

This dramatic increase in phishing and cyberattacks related to COVID-19, and it is not surprising that we also see it now.

Be extremely careful with any emails you received, especially those that are politically or socially motivated, as they could be malware in disguise.

Source: https://www.bleepingcomputer.com/news/security/fake-black-lives-matter-voting-campaign-spreads-trickbot-malware/