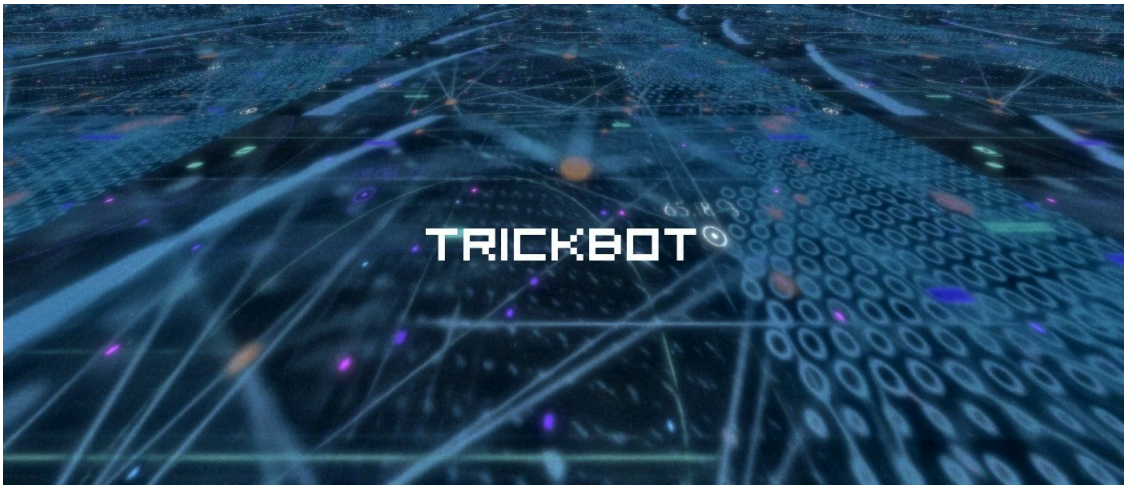
TrickBot phishing checks screen resolution to evade researchers

By Ionut Ilascu

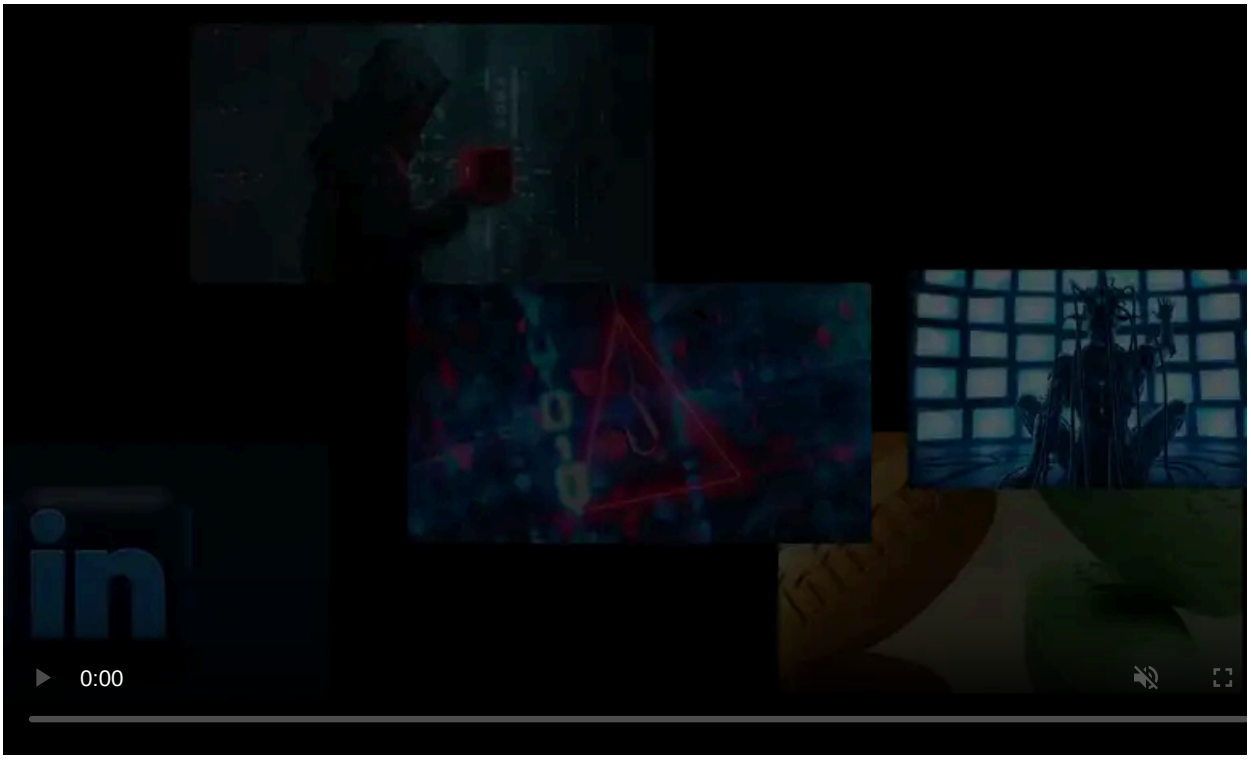
Published: 2021-11-26 · Archived: 2026-04-05 15:43:34 UTC

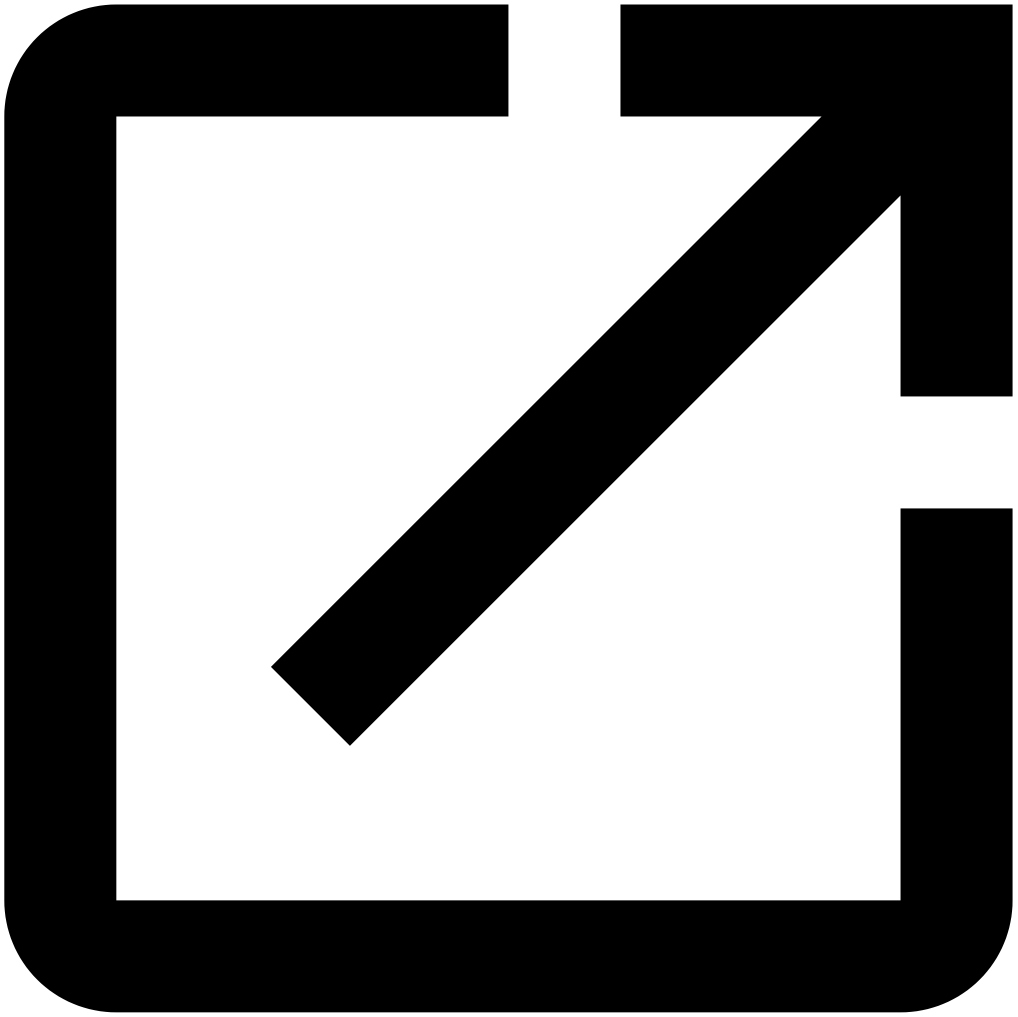


The TrickBot malware operators have been using a new method to check the screen resolution of a victim system to evade detection of security software and analysis by researchers.

Last year, the TrickBot gang added a new feature to their malware that terminated the infection chain if a device was using non-standard screen resolutions of 800x600 and 1024x768.

In a new variation spotted by threat researchers, the verification code has been added to the HTML attachment of the malspam delivered to the potential victim.


0:00



A borrowed trick

Researchers usually analyze malware in virtual machines that come with certain particularities - especially on default configurations - such as running services, name of the machine, network card, CPU features, and screen resolution.

Malware developers are aware of these characteristics and take advantage of implementing methods that stop the infection process on systems identified as virtual machines.

In TrickBot malware samples found last year, the executable included JavaScript code that verified the screen resolution of the system it was running on.

Recently, TheAnalyst - a threat hunter and member of the Cryptolaemus security research group, found that the HTML attachment from a TrickBot malspam campaign behaved differently on a real machine than on a virtual one.

The attachment downloaded a malicious ZIP archive on a physical system but redirected to the ABC's (American Broadcasting Company) website in a virtual environment.

If the target opens the HTML in their web browser, the malicious script is decoded and the payload is deployed on their device.

The email carrying the attachment was a fake alert for purchasing insurance, with details added to an HTML attachment.

Opening the attachment launched the HTML file in the default web browser, displaying a message asking for patience for the document to load and providing a password to access it.

On a regular user’s machine, the infection chain would continue with downloading a ZIP archive that included the TrickBot executable, just as seen in the image below, published by TheAnalyst:

Downloading malware this way is a technique known as HTML smuggling. It allows a threat actor to bypass a browser's content filters and sneak malicious files on a target computer by including encoded JavaScript into an HTML file.

While this appears to be an innovation from TrickBot operators, the trick is not new and has been seen before in attacks luring victims to phishing sites.

Security researcher MalwareHunterTeam found in March this year a phishing kit that included code for checking the system's screen resolution.

Since then, the researcher told BleepingComputer that he saw the tactic being used multiple times in various phishing campaigns as a means to avoid investigators.

The script determines if the user landing on the phishing page uses a virtual machine or a physical one by checking if the web browser uses a software renderer like as SwiftShader, LLVMpipe, or VirtualBox, which typically means that a virtual environment.

As seen above, the script also checks if the color depth of the visitor's screen is less than 24-bits, or if the screen height and width are less than 100 pixels.

TrickBot is not using the same script as the one above but relies on the same tactic to detect a researcher's sandbox. However, it's a premiere for the gang to use such a script in an HTML attachment.

This may also be the first time malware uses an attachment to run a screen resolution check rather than doing it on the landing page serving the malware executable.

Previously, the malware checked for non-standard screen resolutions 800x600 and 1024x768, which are indicative of a virtual machine.

Source: https://www.bleepingcomputer.com/news/security/trickbot-phishing-checks-screen-resolution-to-evade-researchers/