

Alert Bulletin

Bulletin N.:

Publication Date: 13/08/2026

Subject: Alert 2026-88 ClickFix Campaign targeting Mexican users

Traffic Light Protocol (TLP): Amber

Description

A **phishing and social engineering** campaign targeting users in Mexico has been identified, using a supposed **“payment receipt”** and documentation that appears to be related to the **Tax Administration Service (SAT)** as bait.

According to the observed flow and the information provided for this bulletin, the victim receives an email from an **external address belonging to the Gmail domain**, using the subject:

“payment receipt”

The message contains as an attachment a **protected PDF document**, designed to appear as legitimate documentation related to the SAT.

The PDF protection, the tax-related theme, and the institutional appearance of the document seek to increase the credibility of the message and generate enough trust for the victim to continue with the instructions presented.

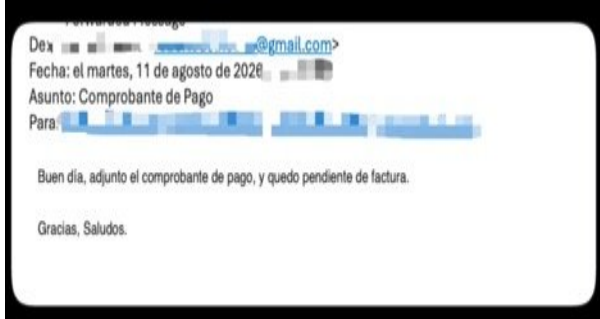
When interacting with the content or with the mechanism included in the document, the victim is led to the next stage of the attack, where a social engineering chain known as **ClickFix** begins.

Unlike traditional attacks that directly exploit a technical vulnerability in the operating system, **ClickFix uses the user themselves to execute the malicious instructions.**

ClickFix is a social engineering technique by which attackers manipulate users into manually executing malicious commands on their own system.

Publicly documented ClickFix campaigns have been used to distribute malware such as **Lumma Stealer, Latrodectus, NetSupport RAT, and DarkGate**, demonstrating that this technique primarily works as a delivery and initial execution mechanism; the final payload may vary depending on the attacker.

It all starts with an email like this “Payment receipt”, supposedly from the SAT.

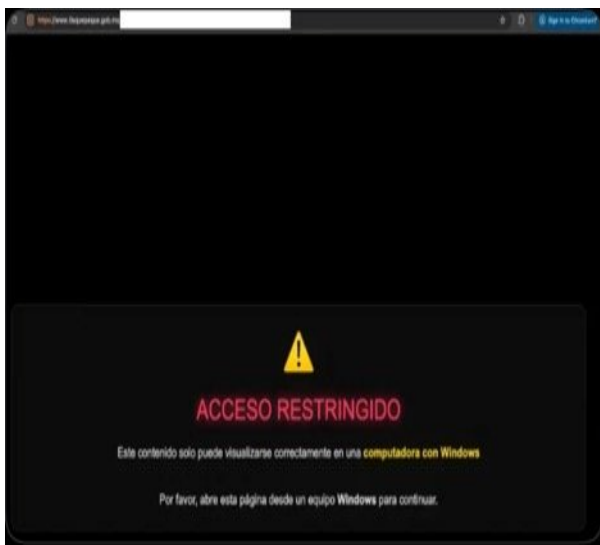


When the user downloads and opens the attached PDF file, it forces the user to click the “Unlock” button



When the user clicks, they are sent to the Government of Tlaquepaque page and there a vulnerability is automatically exploited. This vulnerability sends the user back to another page compromised by the attacker. This page is not from the government, but it is a Mexican site. On that page, another “program” is executed; what you see in the image is the program’s code. This program functions as a police officer; before moving to the second step, it performs a check.

First, it analyzes whether the victim is a program such as an antivirus or programs that exist on the internet that can detect this type of threat. – Then it validates whether the victim uses Windows; if the victim does not use Windows, it shows this screen. This indicates that this attack only works for Windows users. If it is macOS, for example, it shows this screen and the attack ends.



If the victim's computer is Windows, it detects the victim's IP address and sends it to the attackers; if the IP is from Mexico, it sends the message: " *WINDOWS REAL* — Premium target". It also sends the computer's time zone to the attacker. According to the message and the code of the message it sends, we can determine that the attacker uses Telegram or WhatsApp to receive these messages. to arbitrary locations of the host system using the privileges of the user or process that executed docker cp.

Solution

Users and administrators should perform the following actions:

- Do not open unexpected PDF files related to supposed payment receipts.
- Be wary of emails from external accounts claiming to represent the SAT.
- Validate any tax-related communication directly through the official SAT portals.
- Do not execute instructions that request using Windows + R.
- Do not paste commands provided by unknown websites into PowerShell, CMD, or Windows Terminal.

Additional information:

- [Original publication shared on X – @hramcoop](#)
- [Microsoft Threat Intelligence – Think before you Click\(Fix\): Analyzing the ClickFix social engineering technique](#)
- [Palo Alto Networks Unit 42 – Fix the Click: Preventing the ClickFix Attack Vector](#)
- [R3D – Phishing campaigns impersonating the SAT through PDF documents](#)