Check Point Research exposes new versions of the BBTok banking malware, which targets clients of over 40 Mexican and Brazilian banks

By etal

Published: 2023-09-20 · Archived: 2026-04-05 16:02:14 UTC

Highlights:

- Check Point Research (CPR) recently discovered an active campaign deploying a new variant of the BBTok banking malware in Latin America
- Originally exposed in 2020, the newly discovered variant of the malware replicates the interfaces of over 40 Mexican and Brazilian banks, and tricks the infected victims into entering their 2FA code to their bank accounts or into entering their payment card number
- Over the time, the cybercriminals behind the malware are actively maintaining diversified infection chains for different versions of Windows. Those chains employ a wide variety of file types, including ISO, ZIP, LNK, DOCX, JS and XLL
- CPR's findings expose the threat actor's evolution over time, and calls out users to remain alert when entering banking credentials and financial information

BBTok hits LATAM

Check Point Research recently discovered an active campaign operating and deploying a new variant of the BBTok banking malware in Latin America. In the research, we highlight newly discovered infection chains that uses a unique combination of Living off the Land Binaries (LOLBins), resulting in low detection rates, even though this BBTok banking malware has been operating since 2020.

As we analyzed the campaign, we came across some of the threat actor's server-side resources used in the attacks, targeting hundreds of users in Brazil and Mexico.

The server-side components are responsible for serving malicious payloads that were probably distributed through phishing links. We have observed numerous iterations of the same server-side scripts and configuration files which demonstrate the evolution of the BBTok banking malware deployment methods over time.

The evolution of BBTok

The BBTok banking malware, first revealed in 2020, was deployed in Latin America through fileless attacks. The banking malware has a wide set of functionalities, including enumerating and killing processes, keyboard and mouse control and manipulating clipboard contents. Alongside those, BBTok contains classic banking Trojan features, simulating fake login pages to a wide variety of banks operating in Mexico and Brazil.

Since it was first publicly disclosed, the BBTok operators have adopted new TTPs, all while still primarily utilizing phishing emails with attachments for the initial infection. Recently we have seen indications of the banking malware distributed through phishing links, and not as attachments to the email itself.

Since the last public reporting on BBTok in 2020, the operators' techniques, tactics and procedures (TTPs) have evolved significantly, adding additional layers of obfuscation and downloaders, resulting in low detection rates.

BBTok continues being active, targeting users in Brazil and Mexico, employing multi-layered geo-fencing to ensure infected machines are from those countries only.

Multi-layered geo-fencing is a sophisticated approach to creating virtual boundaries or zones in geographic areas. It involves the use of multiple layers of these boundaries, each with its own set of specifications and criteria.

The BBTok banking malware has a dedicated functionality that replicates the interfaces of more than 40 Mexican and Brazilian banks, and tricks the malware victims into entering their 2FA code to their bank accounts or into entering their payment card number. An analysis of the payload server-side code revealed the actors are actively maintaining diversified infection chains for different versions of Windows.

Posing as legitimate institutions, these fake interfaces coax unsuspecting users into divulging personal and financial details, tricking the victim into entering the security code/ token number that serves as 2FA for bank account and to conduct account takeovers of the victim's bank account. In some cases, this capability also tricks the victim into entering their payment card number.

Figure 1 – Examples of fake interfaces embedded within the BBTok Banker

During the research, CPR were able to identify a database of some BBTok malware victims in Mexico, that contained over 150 entries with victims' information:

Figure 2 – Database with victims information

Figure 3 – Geographical distribution of the victims within Mexico

Beware of online phishing attempts

Phishing attacks can have a number of different goals, including malware delivery, stealing money, and credential theft. However, most phishing scams designed to steal your personal information can be detected if you pay enough attention.

Here are a few phishing prevention tips to keep in mind:

1. Always be suspicious of password reset emails

Password reset emails are designed to help when you cannot recall the password for your account. By clicking on a link, you can reset the password to that account to something new. Not knowing your password is, of course, also the problem that cybercriminals face when trying to gain access to your online accounts. By sending a fake password reset email that directs you to a lookalike phishing site, they can convince you to type in your account credentials and send those to them. If you receive an unsolicited password reset email, always visit the website directly (do not click on embedded links) and change your password to something different on that site (and any other sites with the same password).

2. Never share your credentials

Credential theft is a common goal of cyberattacks. Many people reuse the same usernames and passwords across many different accounts, so stealing the credentials for a single account is likely to give an attacker access to a number of the user's online accounts.

As a result, phishing attacks are designed to steal login credentials in various ways, such as:

- **Phishing Sites:** Attackers will create lookalike sites that require user authentication and point to these sites in their phishing emails. Beware of links that do not go where you expect them to.
- **Credential-Stealing Malware:** Not all attacks against your credentials are direct. Some phishing emails carry malware, such as keyloggers or trojans, that are designed to eavesdrop when you type passwords into your computer.
- **Support Scams:** Cybercriminals may pose as customer support specialists from organisations like Microsoft, Apple, and similar companies and ask for your login credentials while they "help" you with your computer.

3. Always note the language in the email

Social engineering techniques are designed to take advantage of human nature. This includes the fact that people are more likely to make mistakes when they're in a hurry and are inclined to follow the orders of people in positions of authority.

Phishing attacks commonly use these techniques to convince their targets to ignore their potential suspicions about an email and click on a link or open an attachment. Some common phishing techniques include:

- **Fake Order/Delivery:** A phishing email will impersonate a trusted brand (Amazon, FedEx, etc.) stating that you have made an order or have an incoming delivery. When you click to cancel the unauthorized order or delivery, the website (which belongs to a cybercriminal) will require authentication, enabling the attacker to steal login credentials.
- **Business Email Compromise (BEC):** BEC scams take advantage of hierarchy and authority within a company. An attacker will impersonate the CEO or other high-level executives and order the recipient of the email to take some action, such as sending money to a certain bank account (that belongs to the scammer).
- **Fake Invoice:** The phisher will pretend to be a legitimate vendor requesting payment of an outstanding invoice. The end goal of this scam is to have money transferred to the attacker's account or to deliver

malware via a malicious document.

Protecting Against Phishing Attacks: To learn more about protecting your organization against phishing, contact us and check out our advanced anti-phishing solution.

Check Point Customers using Threat Emulation and Check Point Harmony Endpoint remain protected against the threat reported in this research

To get the full research visit https://research.checkpoint.com/
