MUST READ: What is a software developer? Everything you need to know about the programmer role and how it is changing

Bizarro banking Trojan surges across Europe

Operators have so far targeted customers of at least 70 banks across Europe and South America.

By Charlie Osborne for Zero Day | May 19, 2021 -- 11:06 GMT (04:06 PDT) | Topic: Security

The Bizarro banking Trojan has targeted customers of at least 70 banks as it moves from its Brazilian base to Europe.

SECURITY

LastPass password manager fine-tunes its multi-factor authentication options (https://www.zdnet.com/article/lastpass-simplifies-its-multi-factor-authentication-app/)

Cyber security 101: Protect your privacy from hackers, spies, and the government (https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/)

The best antivirus software and apps (https://www.zdnet.com/article/best-antivirus/)

The best VPNs for business and home use (https://www.zdnet.com/article/best-vpn/)

The best security keys for two-factor authentication (https://www.zdnet.com/article/best-security-key/)

Colonial Pipeline attack: What happened (ZDNet YouTube) (https://www.youtube.com/watch?v=xyyMRMM6BOo)

This week, Kaspersky researchers said the Trojan variant (https://securelist.com/bizarro-banking-trojan-e[illegible]-europe/102258/), originating in Brazil -- as many seem to do

(https://www.zdnet.com/article/banking-trojan-evolves-from-distribution-through-porn-to-sophisticated-phishing-schemes/) -- is now striking users in not only in Brazil, but Argentina, Chile, Spain, Portugal, France, and Italy, with customers of banks in these areas being lured into handing over their account credentials for the purposes of financial theft.

However, the attack chain isn't purely digital, as money mules are used at the end of a successful compromise to cash out funds or transfer stolen money.

The banking Trojan, likened to the "Tetrade (https://securelist.com/the-tetrade-brazilian-banking-malware/97779/)" family of four strains running rampant across Brazil, is distributed via spam emails containing an MSI installer package.

Social engineering is performed to try and fool potential victims into accepting and executing the installer including by way of messages pretending to be tax notifications and alerts.

Once launched, the installer downloads a .ZIP archive fetched from a compromised website or server. The researchers have found Azure and AWS servers that were used to host the malware, alongside hijacked WordPress domains.

The archive contains a malicious .DLL, written in Delphi, a AutoHotkey script runner executable, and a script that calls an exported function from the .DLL. This function, which is obfuscated, contains the malicious code required to trigger the banking Trojan.

On startup, Bizarro will kill existing browser processes, including any active sessions with online banking services. As soon as the victim restarts their session, bank credentials are quietly captured by the malware and sent to an attacker's command-and-control (C2) server.

To improve the chances of capturing this valuable data, Bizarro also disables autocomplete functionality in a browser.

Fake pop-ups are also shown to users, some of which are tailored to appear as messages from online banking services warning of security updates or PC compromise. These pop-ups may freeze PCs and hide taskbars, while at the same time, requesting identity checks by the client.

This is where a second-stage attack comes into play. The messages will try and lure victims in[illegible]o-factor authentication (2FA) codes -- when this security measure is enabled

-- by asking them to download a malicious smartphone app and scanning a QR code for 'authentication' purposes.

The malware will capture operating system information and is also able to perform screen captures, keylogging, and will monitor clipboards for cryptocurrency wallet addresses.

If any are detected, wallet addresses are replaced by those owned by the threat actors in the hopes that the victim may unwittingly transfer cryptocurrency.

As a Trojan, Bizarro also contains backdoor functionality that manages the C2 connection.

This is not the only banking Trojan from Brazil that has expanded to other regions. Now joining the likes of (https://www.zdnet.com/article/meet-janeleiro-a-new-banking-trojan-striking-corporate-targets/) Guildma, Javali, Melcoz, and Grandoreiro, the operators are expected to continue striking targets in multiple countries, as well as continue to improve their malware over time.

PREVIOUS AND RELATED COVERAGE

- Meet Janeleiro: a new banking Trojan striking company, government targets (https://www.zdnet.com/article/meet-janeleiro-a-new-banking-trojan-striking-corporate-targets/)
- Banking Trojan evolves from distribution through porn to phishing schemes (https://www.zdnet.com/article/banking-trojan-evolves-from-distribution-through-porn-to-sophisticated-phishing-schemes/)
- New Android malware targeting banks in Italy, Spain, Germany, Belgium, and the Netherlands (https://www.zdnet.com/article/new-android-malware-targeting-banks-in-italy-spain-germany-belgium-and-the-netherlands/)

Have a tip? Get in touch securely via WhatsApp | Signal at +447713 025 499, or over at Keybase: charlie0

RELATED TOPICS: SECURITY TV | DATA MANAGEMENT | CXO | DATA CENTERS

By Zero Day | May 19, 2021 -- 11:06 GMT (04:06 PDT) | Topic: Security