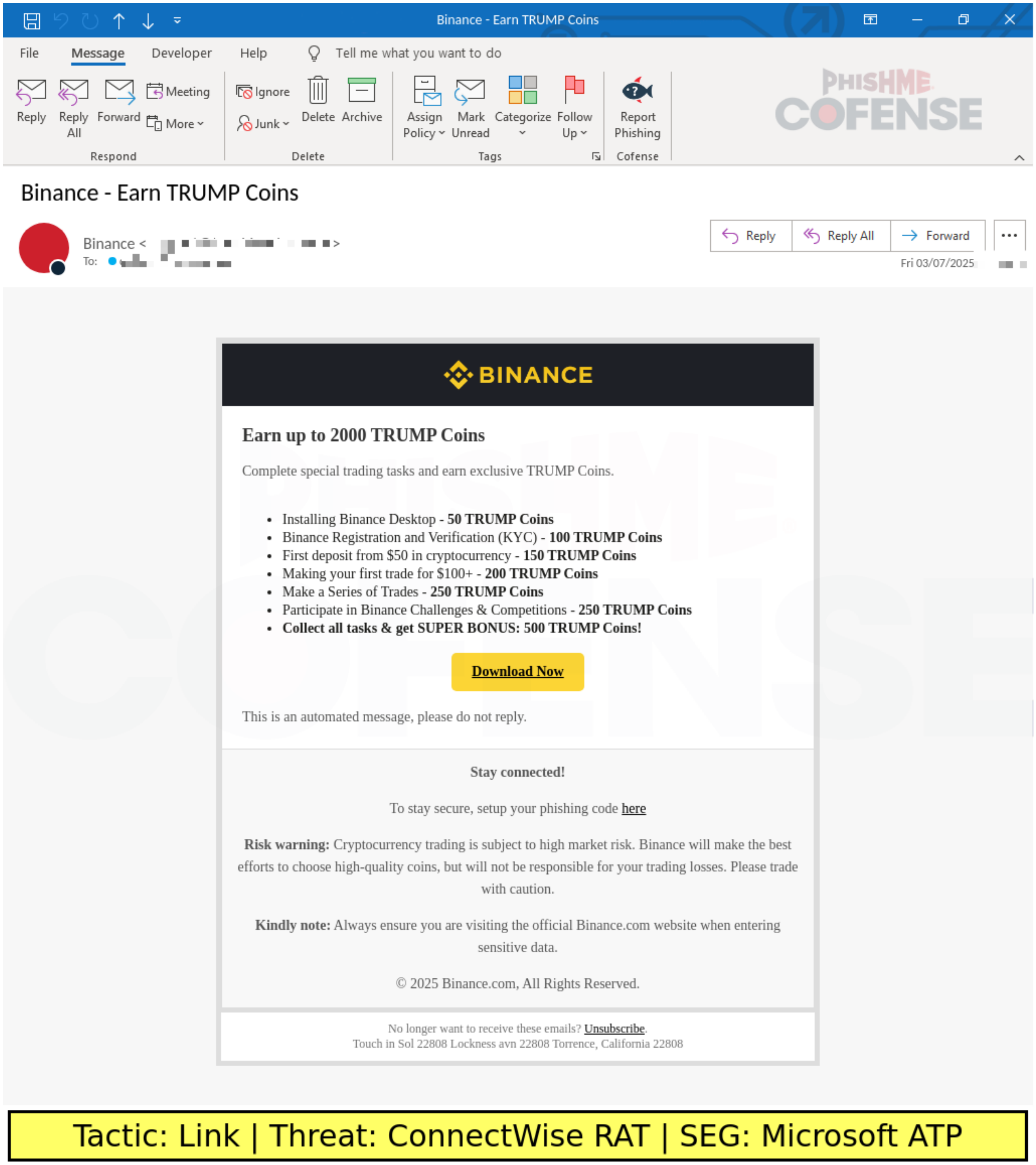
Trump Cryptocurrency Delivers ConnectWise RAT

cofense.com/blog/trump-cryptocurrency-delivers-connectwise-rat

March 10, 2025

Author: Max Gannon, Intelligence Team

An email campaign spoofing Binance claims to deliver an opportunity to claim recently created TRUMP coins. If victims follow the instructions and download “Binance Desktop” in order to get TRUMP coins they instead install ConnectWise RAT. The threat actors behind this campaign are eagerly monitoring infections and can connect to infected computers in under 2 minutes.



Binance - Earn TRUMP Coins

Binance < [redacted] >
To: [redacted]

Fri 03/07/2025 [redacted]

BINANCE

Earn up to 2000 TRUMP Coins

Complete special trading tasks and earn exclusive TRUMP Coins.

- Installing Binance Desktop - **50 TRUMP Coins**
- Binance Registration and Verification (KYC) - **100 TRUMP Coins**
- First deposit from $50 in cryptocurrency - **150 TRUMP Coins**
- Making your first trade for $100+ - **200 TRUMP Coins**
- Make a Series of Trades - **250 TRUMP Coins**
- Participate in Binance Challenges & Competitions - **250 TRUMP Coins**
- **Collect all tasks & get SUPER BONUS: 500 TRUMP Coins!**

Download Now

This is an automated message, please do not reply.

Stay connected!

To stay secure, setup your phishing code here

Risk warning: Cryptocurrency trading is subject to high market risk. Binance will make the best efforts to choose high-quality coins, but will not be responsible for your trading losses. Please trade with caution.

Kindly note: Always ensure you are visiting the official Binance.com website when entering sensitive data.

© 2025 Binance.com, All Rights Reserved.

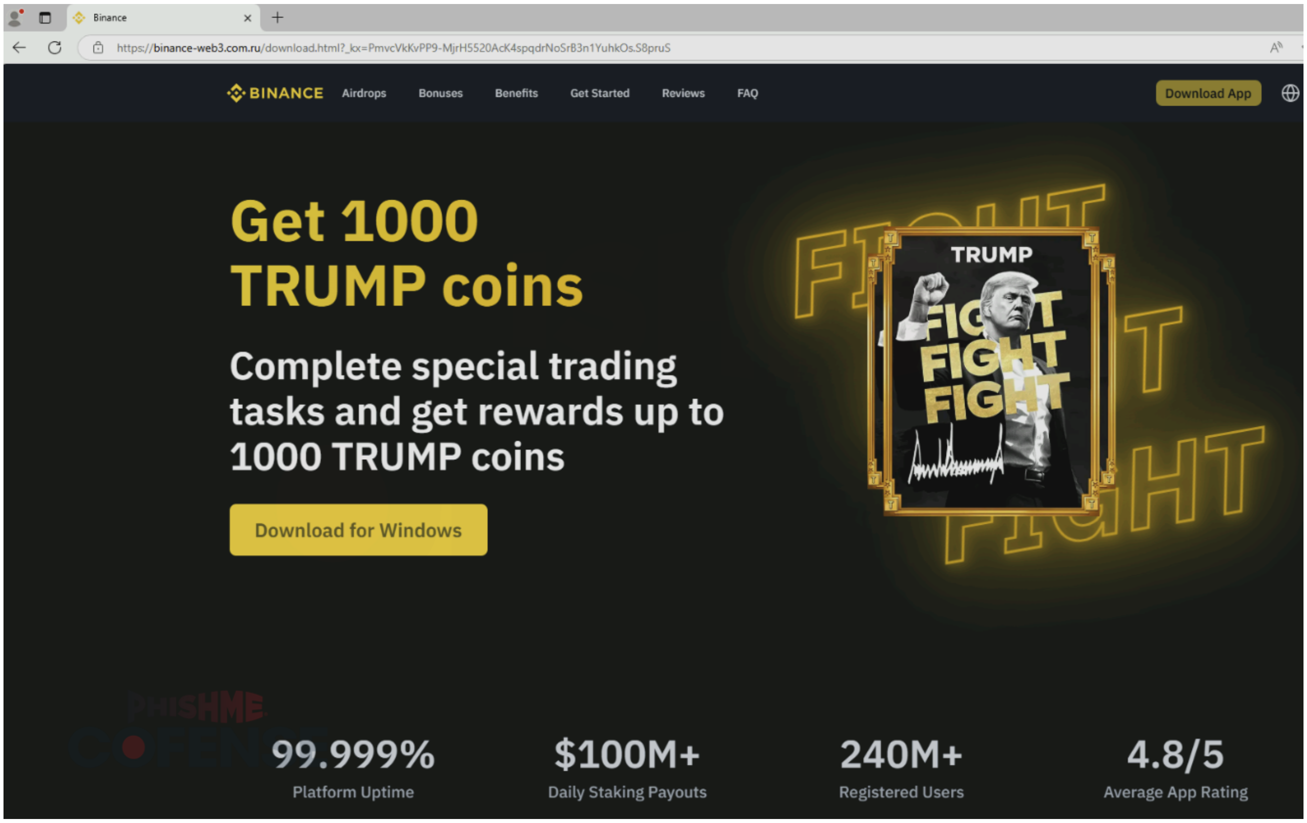
No longer want to receive these emails? Unsubscribe.
Touch in Sol 22808 Lockness avn 22808 Torrence, California 22808

Tactic: Link | Threat: ConnectWise RAT | SEG: Microsoft ATP

Figure 1: Email spoofing Binance to deliver ConnectWise RAT.

This campaign took several steps to impersonate Binance, such as using “Binance” as the sender’s name and including a “risk warning” in the email, which is more likely to make people trust that it is legitimate. The threat actors also took great pains to make the website hosting the ConnectWise RAT download appear legitimate, as can be seen in Figure 2.

Although they did not directly copy the Binance TRUMP coin page or the Binance client download page, the threat actors combined images from both into a convincing page which included further install steps farther down.



https://binance-web3.com.ru/download.html?_kx=PmvcVkKvPP9-MjrH5520AcK4spqdrNoSrB3n1YuhkOs.S8pruS

Get 1000 TRUMP coins

Complete special trading tasks and get rewards up to 1000 TRUMP coins

99.999% Platform Uptime

$100M+ Daily Staking Payouts

240M+ Registered Users

4.8/5 Average App Rating

Figure 2: Web page hosting ConnectWise RAT installer download.

The download link which purports to lead to a Binance desktop client instead downloads the installer for ConnectWise RAT. This sample of ConnectWise RAT connects to a C2 which is actively monitored by a threat actor. Shortly after checking in, the threat actor takes remote control of any infected computers. This is in contrast to most ConnectWise RAT installations where the threat actor will only decide to interact with an infected host after some time has passed. After a threat actor has connected, they will target saved passwords for applications such as Microsoft Edge, making up for ConnectWise RAT’s relative lack of information theft capabilities.

Table 1: IOCs for this campaign

IOC	Purpose
hxxps[://]ctrk[.]klclick2[.]com/l/01JNRGM3JYQC3X8C47X9EN8SER	URL embedded in email

hxxps[://]binance-web3[.]com[.]ru/download[.]html	Website hosting download link
hxxps[://]binance-web3[.]com[.]ru/BinanceSetup[.]exe	URL used to download ConnectWise RAT
shopifycourses[.]store:8041	ConnectWise RAT C2

Following the identification of this phishing scheme by the Cofense Intelligence team, it was added as a PhishMe Security Awareness Training simulation. Organizations using PhishMe SAT can now equip their employees to spot threats like the Trump Bitcoin cryptocurrency scam, even if such attacks manage to bypass perimeter defenses.

To learn more about how Cofense utilizes phishing scams that have been identified by our Intelligence team to train your employees on real and relevant threats, schedule a demo with a member of our team.