Intelligence Alert

CSA-240331

Chinese Threat Actor Aims to Monetize Phishing Through Payment Gateway Fraud

CROWDSTRIKE INTELLIGENCE

CROWDSTRIKE

This report is provided for situational awareness and network defense purposes only. DO NOT conduct searches on, communicate with, or engage any individuals, organizations, or network addresses identified in this report. Doing so may put you or your employer at risk and jeopardize any ongoing investigation efforts.

PROPRIETARY AND CONFIDENTIAL • NOT TO BE SHARED WITH THIRD PARTIES • COPYRIGHT 2024

CSA-240331

Chinese Threat Actor Aims to Monetize Phishing Through Payment Gateway Fraud

Publish Date: 18 March 2024

Summary

In March 2024, a highly likely China-based threat actor using the moniker 大仔 (pronounced dazai) claimed to have recently acquired a large volume of carding data through phishing activity targeting Europe, then solicited U.S.-based payment gateway accounts to monetize the data through payment gateway fraud.

Prior to advertising the need for new collaborators, the threat actor had reportedly used payment gateway fraud with two U.S.-based individuals' accounts for two years, but those individuals recently rescinded their collaboration due to fear of legal consequences.

Details

In March 2024, the threat actor operating the China-based moniker *dazai* solicited U.S.-based payment gateway account holders to collaborate in payment gateway fraud.[1] The threat actor claims to sell Phishing-as-a-Service (PHaaS) infrastructure that primarily targets U.S. and European victims. Specifically, *dazai* stated that their phishing activity usually aims to collect the victim's name, phone number, email address, physical address, payment card numbers, credit card verification (CCV) code, payment environment, and device fingerprint (Figure 1).

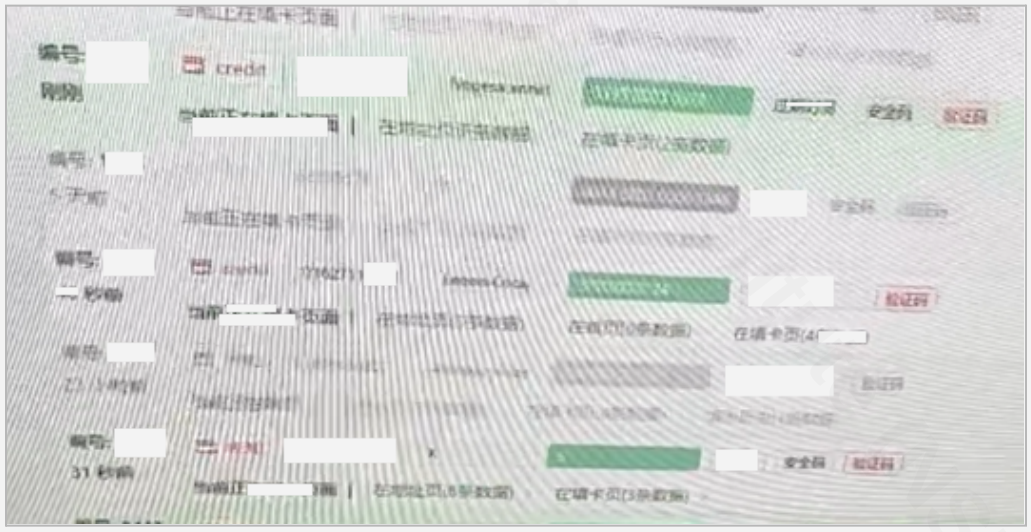

Figure 1. Payment Card Data Allegedly in dazai's Possession

[1] Generally, threat actors commit payment gateway fraud by creating a fraudulent business that can receive card payments through logins to a payment gateway account. After completing the transactions for nonexistent goods or services, the payment gateway account owner withdraws the money. This collaborator often then returns a predetermined portion of the money to the threat actor.

Copyright 2024

Although specific details about the methods *dazai* uses to complete payment gateway fraud remain limited, the actor's advertisement reveals multiple elements of their process. The advertisement indicates that *dazai* seeks accounts registered prior to 2022 that have a demonstrated payment history, as an established account is less likely to draw scrutiny from authorities than a new account. Additionally, *dazai* alleges to conduct transactions totaling about $5,000 USD per day per payment gateway account; potential collaborators are expected to return 50 percent of all transactions to *dazai* in Tether (USDT).

Antifraud systems typically evaluate digital fingerprints and payment environments surrounding payment card transactions[2]; however, *dazai* claims to have created an algorithm that mimics the legitimate digital fingerprints and payment environments collected during phishing. Moreover, *dazai* advertises point-of-sale (POS) equipment for sale, indicating that they have access to equipment that can be used to complete these fraudulent transactions (Figure 2).

Figure 2. POS Device Allegedly in dazai's Possession

Threat actors often advertise payment gateway accounts on underground marketplaces and in eCrime-focused Telegram channels, usually for the purpose of conducting cashouts. Additionally, CrowdStrike Intelligence has previously observed a West African eCrime group soliciting payment gateway accounts to perform cashouts (CSIT-21078).

[2] https[:]//nethone[.]com/blog/digital-fingerprinting-in-fraud-detection-part-1-intro

Copyright 2024