JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP: AMBER+STRICT

Product ID: AA24-032A

February 1, 2024

China-Based Actors Conducting Unemployment Compensation Fraud Targeting US States

SUMMARY

The Federal Bureau of Investigation (FBI) and the US Department of Labor, Office of Inspector General (DOL-OIG) observed new efforts by presumed China-based actors to target unemployment compensation benefits through high-velocity, automated cyber activity against state departments and agencies responsible for the disbursement of such funds. FBI and DOL-OIG intend to raise awareness of this ongoing activity and recommend mitigation measures to US state labor departments and workforce agencies and other affected entities along with information technology professionals.

The FBI and DOL-OIG associated this activity with previous fraudulent activity originating from China, which targeted unemployment compensation benefits and COVID-19 pandemic relief funds from several US state governments between January 2021 and March 2022. These unemployment compensation claims transferred to bank accounts previously set up online using presumed stolen US person personally identifiable information (PII). During that timeframe, deposits into fraudulent accounts were mostly of similar dollar amounts. The actors

ACTIONS TO TAKE TODAY

- Search for indicators of compromise, and report newly-identified activity.
- Enforce the principle of least privilege.
- Implement multifactor authentication.
- Implement identity verification mechanisms for new account registrations and mergers.
- Adjust firewall rules to detect outdated or irregular user-agent strings originating from proxies or China.
- Adjust firewall rules to detect the use of proxies and activities outside of normal business hours.
- Implement signature and heuristics analysis to detect bot-automated account openings.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact the Cybersecurity and Infrastructure Security Agency (CISA) at CISAServiceDesk@cisa.dhs.gov.

This document is marked TLP: AMBER+STRICT. Disclosure is limited to only individuals within the recipient organization. Sources may use TLP: AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP: AMBER+STRICT information with members of their own organization, but only on a need-to-know basis to protect their organization and prevent further harm. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

laundered these funds through a series of US-based bank accounts and related US-based shell companies until the funds transferred to unidentified entities in China.

FRAUDULENT CLAIMS AND STATE GOVERNMENT ACCOUNTS

Beginning in November 2022, several identified US state workforce agencies experienced new increases in unemployment compensation fraud and attempted fraud activity. In March 2023, an identified US state encountered high-velocity unemployment compensation fraud activity stemming from newly created accounts that exploited a security flaw where users could link new accounts to existing social security numbers (SSNs) and unemployment compensation claims. The threat actors attempted to carry out the following actions:

- Establishing new unemployment compensation claimant accounts;
- Accessing pre-existing unemployment compensation claimant accounts, including accounts of state government employees;
- Making changes to direct deposit information, often to banks with no in-state presence or routing numbers that correspond to other regions;
- Establishing new employer accounts;
- Accessing pre-existing employer accounts, including accounts established by Third Party Administrators administering unemployment compensation benefits for hundreds to thousands of employees, particularly in the healthcare industry; and
- Fraudulently filing for pandemic and post-pandemic (regular) unemployment compensation benefits.

State-level information security personnel indicated that cyber criminals rapidly accessed unemployment compensation web applications, potentially through automation, and readily defeated common knowledge-based identity verification tools. Additionally, actors made hundreds of thousands of requests against unemployment compensation web applications over brief periods. In some instances, the actors appeared to possess specific internal field names from state unemployment compensation databases.

TECHNICAL DETAILS

Throughout the existence of this activity, the actors employed a series of tactics, techniques, and procedures (TTPs) to automate their unemployment compensation fraud scheme:

- Using proxies to spoof their location to a specific city and state in the United States where they were opening online bank accounts and submitting unemployment compensation claims and to mask their true location;
- Automating the account opening and unemployment compensation claim submission processes to allow for bulk account openings and claim submissions;
- Using automation frameworks and tools to facilitate the acquisition and transfer of funds;
- Employing anti-detect browsers to create unique digital fingerprints to avoid detection; and
- Using verification tools to confirm account openings and registrations.

Residential Proxy Services

The China-based actors employed a series of proxy services to virtually geolocate themselves to a specific city and state in the United States, where they were opening online bank accounts and submitting unemployment compensation claims. This allowed the actors to mask their true location.

China-based actors employed the 911S5 residential proxy service, until the platform was taken offline by the administrator in July 2022. The platform offered a pay-per-connection model, which allowed customers to access and connect to computers around the world. The platform allowed users to obfuscate the actual origination of internet traffic and make it appear that a victim computer had been the origination of any online internet traffic. After 911S5 ceased operations, traffic related to the unemployment compensation fraud activity indicated potential usage of the Luminati proxy service.

Automated Bank Account Openings

To obtain the fraudulent UC claims from various states, the actors opened online bank accounts at multiple US financial institutions in bulk. They used these accounts to launder the funds through a series of transfers until they reached accounts associated with front companies connected to Chinese nationals. Bank accounts were created in batches through "bot-generated" activity starting in mid-March 2022, which used residential proxy services. The transfers avoided fraud detection thresholds by maintaining minimal account balances and conducting smaller payments to avoid overdraft.

Automated Batch Bank Account Opening Characteristics

The accounts opened through batch automation had the following features:

- Used stolen PII from specific US states for multiple account openings around the same time;
- Used a residential proxy service IP address to match the bank account opening to a specific city and state that matched the stolen PII;
    - Some account openings were associated with China-based IP addresses;
- Single user, no debit card, and no direct deposits;
- Machine-generated online IDs (identified through a pattern-based token conversion), with small windows of enrollment dates;
- Outdated Windows OS (e.g., Windows Vista, 7, 8 and 8.1), user-agent strings with randomized data non-matching common browsers, and older NVIDIA graphics cards. Other bank account opening applications used iOS 14;
- Copy and paste or automatic-fill functions through scripts or automation applications;
- High volumes of online account applications with the same secret question and answer;
- High volumes of online account applications with similar listed occupations, with "salesperson" or "unemployed" being most common;
- Browser language set to English, although some were set to Chinese; and
- Similar username patterns using a first name with a string of seven characters and attempts to link the accounts to external financial institutions.

Automation Applications

Threat actors based in China employed a variety of automation tools and applications to increase the velocity of online bank account openings, state unemployment compensation account openings, and unemployment compensation claims. The actors also used automation tools to track their unemployment compensation claims and payments to various bank accounts. For example, the actors used Puppeteer in combination with anti-detect browser services, such as Multilogin, to circumvent fingerprinting detection.

Anti-Detect Browsers

China-based actors used anti-detect browsers such as Multilogin[1] and AdsPower[2] to manage multiple browser profiles, create unique digital fingerprints to circumvent detection, and obfuscate their identities. These browsers also support automation frameworks as described above, allowing the actors to combine and integrate tools by using application programming interfaces (APIs) and scripts. Login notifications revealed IP addresses resolving to Sichuan Province, China.

Verification Tools

Threat actors employed multiple services designed to verify online identities or to forge official paperwork for unemployment compensation claims, online accounts, and banking transactions that required using stolen US persons' PII. These tools enabled the actors to obtain templates for driver's licenses for multiple US states, multiple US tax forms, and US certificates of incorporation. The actors also used various tools for SMS verification for online accounts.

MITIGATIONS

The FBI and DOL-OIG encourage the banking sector, and financial organizations, to:

- Identify anomalies within the account opening procedures within your institution.
- Search for indicators of compromise, and report newly identified activity.
- Log DNS queries and consider blocking all outbound DNS requests that do not originate from approved DNS servers. Monitor DNS queries for C2 over DNS or other data exfiltration over DNS. *Reminder: based on the TTPs employed by the actor to maintain persistence (e.g., C2DD), initial, outright blocking of IOCs is likely not an effective way to address this activity. Organizations should consider taking steps to understand the full extent of an ongoing compromise before blocking associated malicious infrastructure.*
- Enforce the principle of least privilege.
- Implement multifactor authentication.
- Implement identity verification mechanisms for new account registrations and mergers. Implement internal security controls, to include training for customer service personnel.

[1] Multilogin is an anti-detect browser that lets the user create multiple unrelated profiles, each with its own unique digital fingerprint through physical device simulation. Additionally, Multilogin has an API and can integrate automation frameworks such as Puppeteer.
[2] AdsPower is a Chinese anti-detect browser aimed at managing e-commerce and social media accounts. The browser offers powerful automation features that require no programming knowledge.

- Adjust firewall rules to detect outdated or irregular user-agent strings originating from proxies or from China-based IP addresses.
- Adjust firewall rules to detect the use of proxies and activities outside of normal business hours. Implement signature and heuristics analysis to detect bot-automated account openings.
- Use endpoint detection and response (EDR) tools. Many of these tools go beyond signature-based detection mechanisms, allow a high degree of visibility into the security status of endpoints, and can be an effective defense against threat actors. EDR tools are particularly useful for detecting lateral movement, as they have insight into common and uncommon network connections for each host.
- Engage with state workforce agency fraud and benefit control personnel to build cyber identifiers into traditional fraud detection methodology for unemployment compensation claims.

CONTACT

This product was coauthored by FBI and DOL-OIG and coordinated with the Cybersecurity and Infrastructure Security Agency (CISA). Recipients of this report are encouraged to contribute any additional information that they may have related to this threat.

For any questions related to this report or to report an intrusion and request resources for incident response or technical assistance, please contact:

- The FBI through the FBI Cyber Division (855-292-3937 or CyWatch@fbi.gov), or a local field office, and the Internet Crime Complaint Center (www.ic3.gov)
- DOL-OIG (https://www.oig.dol.gov/hotline.htm)