Termination of Federal Unemployment Programs Represents Turning Point for Fraudsters

recordedfuture.com/termination-federal-unemployment-programs-turning-point-fraudsters/

Insikt Group

Since early 2020, Recorded Future has continued to witness prominent changes within underground communities in response to COVID-19 including an interest in defrauding government entities via fraudulent unemployment benefit applications. As detailed in our general reporting on the threat landscape of unemployment fraud earlier this year, criminals continued to use a variety of methods with relative ease, contributing to a growing marketplace that saw topics such as Pandemic Unemployment Assistance (PUA) appear as a sub-category within underground marketplaces that offered fraudulent tutorials or methods for aspiring criminals. In addition to these tutorials, we occasionally observed the sale of compromised account information that came bundled with tutorials on how to best profit off the stolen information. This past month, however, has served as a critical turning point for this general landscape with The CARES Act and other federal programs that provided unemployment benefits for many claimants having expired the week of September 4, 2021. The federal PUA program provided unemployment benefits to individuals not eligible for regular unemployment compensation or extended benefits, including those who have exhausted all rights to such benefits. Recorded Future analysts have monitored for changes since September 4 and noted the following:

- Despite the termination of federal programs, references to PUA guides and methods continue to persist. It is certainly possible that this is either a combination of ignorance on the part of some criminal entities who were initially unaware that the federal programs had ended or were attempts to scam other criminals operating on these sources for a quick profit.
- Although the PUA program expired in September 2021, the methods used by the actors to brute force accounts on these government websites, combined with the relative ease with which actors can steal funds intended for US citizens, indicate that similar government assistance programs may be targeted in the future.

- Fraudsters are attempting to use their alleged experience in orchestrating PUA fraud schemes to demonstrate their ability to perform other forms of fraud that are likely to persist, such as those targeting other government assistance or loan programs. Some actors have implied they intend to shift their targeting to other programs that have proven reliable throughout the pandemic such as those targeting US Small Business Administration (SBA) relief efforts.
- Recorded Future has continued to observe criminal marketplaces that specialize in the sale of stolen credentials routinely reference pandemic unemployment platform login information for sale at low cost. The exposure of this login information for individual account balances is still relevant even after the termination of federal programs for individuals who have remaining relief balances or fail to maintain proper security hygiene by reusing the same password across multiple platforms. Other effects of a victim logging into an account whose login information was compromised may enable actors responsible for the compromise to steal additional personally identifiable information (PII), including bank account information.

Figure 1: *Breakdown of Fraud Methods Available for Purchase (October 15, 2021), Source: Telegram*

Some actors have been very frank in their description of what the future of PUA fraud holds within closed access sources, leaving comments such as: *"Pua is dead already, just like the sba, now only loans work".* However, other actors have continued to promote the sale of methods or tutorials both before and after the September federal deadline, clearly noting that some methods are very unlikely to be as profitable once the programs were terminated. In some advertisements actors appear to be unperturbed by the termination of the programs, advertising "NEW" working methods for multiple states. The methods used by the actors, as well as the underlying vulnerabilities in the platforms used by certain states' PUA websites, can likely be replicated for broader targeting. In some observed scenarios, threat actors specifically stated they had acquired stolen login credentials for PUA accounts through routine attack vectors such as brute-force attacks.

Figure 2: *Actor Urging Members to Use an Ohio Method of PUA Fraud Before the September 2021 Federal Deadline Passed, Source: Telegram*

Cybercriminals used brute-forced login credentials and stolen personally identifiable information (PII) bundled as packages of 'fullz' (sets of data on individuals that typically includes full names, Social Security Numbers, addresses, account numbers, and birthdays) to compromise victims' PUA accounts. More broadly, actors have also continued to sell methods in which criminals can access unemployment relief balances for certain states. However, prior analysis of several PUA tutorials by Recorded Future's Gemini Advisory confirmed that these actors have occasionally expressed doubts about some methods' viability due to factors such as a large number of potential victims possibly having already submitted a claim for payment through PUA or other actors may have already attempted to brute force the account password.

Regardless of the status of these now-defunct federal programs, the effect that the scale of stolen PII or login credentials from unemployment platforms has had on the criminal underground is also likely to persist. Recorded Future has continued to observe more automated criminal marketplaces that specialize in the sale of stolen credentials routinely referencing pandemic unemployment platform login information for sale at low cost. The exposure of this login information for individual account balances is still relevant even after the termination of federal programs for individuals who have remaining balances or fail to maintain proper security hygiene by reusing the same password across multiple platforms. The average cost of listings from shops such as the one below doesn't exceed $10, representing the ease to which actors who are either unable to have no desire to learn about PUA-specific methods, such as brute forcing, can instead opt to outright purchase login credentials to perform unauthorized actions within a victim's account.

 ***Figure 3:*** *Underground Marketplace Advertisement for Stolen Ohio Unemployment Login Data (September 26, 2021), Source: Amigos Market*

The visual in Figure 1 provides an example of other forms of fraud that are likely to continue to be of interest in the near future to criminals already beginning to adapt to the transition that the closure of the PUA federal program has brought. We anticipate that criminals will continue to target PUA account balances that are still in the process of filing claims even after the federal deadline due to exceptions that may have been granted to individuals who had their claims frozen or put on indefinite hold. This was a relatively common event over the past year given the massive volume of PUA claims placed into a backlog status by state governments who had to contend with the task of sorting fictitious claims from legitimate ones. More broadly, although the PUA program expired in September 2021, the methods used by the actors to brute force accounts on these government websites, combined with the relative ease with which actors can steal funds intended for US citizens, indicate that similar government assistance programs may be targeted in the future. Figure 4 below shows the overall fluctuation in mentions of either "PUA" or "SBA" within underground sources monitored by Recorded Future, with the volume of posts closely mirroring one another given how intertwined promotions for these services are within the same posting. Another point of consideration is the sudden uptick in discussion within several threads even after the termination of the federal programs for both topic areas.

  ***Figure 4:*** *Comparison Between References to "PUA" (Upper) & "SBA" (Lower) Within Underground Sources (Past 60 Days), Source: Gemini Advisory Data*