The Nigerian fraudsters ripping off the unemployment system

reader comments

32 with 23 posters participating

Share this story

As millions of people around the United States scrambled in recent weeks to collect unemployment benefits and disbursements through the federal CARES Act, officials warned about the looming threat of COVID-19-related scams online. Now they're here.

Last Thursday, the Secret Service issued an alert about a massive operation to file fraudulent unemployment claims in states around the country, like Washington and Massachusetts. Officials attributed the activity to Nigerian scammers and said millions of dollars had already been stolen. New research is now shedding light on one of the actors tied to the scams—and the other pandemic hustles they have going.

The email security firm Agari today will release findings that an actor within the Nigerian cybercriminal group Scattered Canary is filing fraudulent unemployment claims and receiving benefits from multiple states, while also receiving CARES payouts from the Internal Revenue Service. So far, this has netted hundreds of thousands of dollars in scam payments. Regular unemployment, the extra $600 per week that out-of-work Americans can claim during the pandemic, plus the one-time

$1,200 payment eligible adults are receiving under the CARES Act are all vulnerable targets for cybercriminals. In the midst of a pandemic and critical economic downturn, though, the theft of those benefits could have particularly dire consequences. The Secret Service warns that hundreds of millions of dollars could be lost to such scams just as states are running out of money to fund unemployment on their own.

The Secret Service says that scammers are using stolen personal information to file the fraudulent relief claims, similar to how they perpetrate tax fraud year to year. The Agari researchers add that the personal data fraudsters are using right now, like home addresses and Social Security numbers, may come not only from ancient data breaches but from a spike in payroll data theft in March and April. When scammers claim unemployment benefits in someone's name, they are either getting to the money before the victim has a chance to or are filing on behalf of people who haven't actually lost their jobs. In the case of the one-time CARES Act payments, scammers are submitting through the special "non-filers" IRS category to divert those payments into their own pockets. Agari researchers say that Scattered Canary has filed at least 82 CARES claims, of which 30 were accepted by the IRS.

"We can't 100 percent confirm that the Scattered Canary actors we're looking at are the actors the Secret Service is referring to, but at least one of these actors is committing unemployment fraud against the states of Washington and Massachusetts," says Crane Hassold, Agari's senior director of threat research and a former digital behavior analyst for the Federal Bureau of Investigation. "They're also involved in committing fraud against CARES payments."

From Florida to Wyoming

In addition to those two states, the Secret Service said it also sees evidence of attacks in North Carolina, Rhode Island, Oklahoma, Wyoming, and Florida. Agari researchers say that Scattered Canary has filed at least 174 fraudulent unemployment claims in Washington since April 29 and 17 fraudulent claims in Massachusetts on May 15 and 16 that were all accepted. This is consistent with the Secret Service's warning that Washington has been hit hardest by scam campaigns. Over time, Agari calculates that all of those claims combined could pay out as much as $5.4 million if they aren't blocked. On Sunday evening, a Scattered Canary actor also filed a fraudulent unemployment claim in Hawaii. Agari says it was accepted.

The IRS did not return a request from WIRED for comment. The Hawaii Unemployment Insurance Special Activities Unit could not be reached for comment.

"The United States Secret Service Global Investigative Operations Center along with our Electronic Crimes Task Force partners have identified criminal actors targeting state unemployment insurance program funds," a Secret Service spokesperson said in a statement. "Criminals will use stolen personally identifiable information to file fraudulent state unemployment claims. The Secret Service's primary investigative priorities are to mitigate any attempts by criminals that target citizens for identity theft and cyber-enabled crimes as it relates to COVID-19."

"Business email compromise"

Scattered Canary is a full-service "business email compromise" operation that uses scams like email impersonation and phishing to manipulate businesses into paying out phony contracts and other fake invoices. Then Scattered Canary uses

a network of money mules within the United States and around the world to route the money. BEC fraudsters participate in a wide variety of hustles—from Craigslist rental scams to payroll data theft and snagging people's tax refunds—to make money and build out a sort of scam toolkit.

"Scattered Canary has committed unemployment fraud along with a number of other government services-focused frauds like disaster relief fraud, Social Security fraud, and student aid fraud," Agari's Hassold says. "Many West African scam groups have also been heavily involved in other incidents, like W-2 BEC attacks, where they can harvest a significant amount of personal information, so it's not surprising they have the information needed to carry out these attacks on unemployment services."

In Scattered Canary's recent rash of unemployment and CARES payment fraud, the researchers say that the group is using a technique it has leaned on in the past to keep track of all its fraudulent unemployment submissions. The scammers will set up one generic-looking Gmail address and then make accounts to submit fraudulent claims adding periods into different parts of the address. Most Web platforms will interpret all of these as different email accounts, while Gmail doesn't recognize periods as changing its own addresses. As a result, the scammers can file dozens of individual submissions under as many people's names, using their specific personal information, while managing it all from one centralized email account. One campaign the Agari researchers analyzed used 259 variations of the same address.

Taking advantage

Once scammers get the government to pay out, a Secret Service spokesperson said that they "use social engineering techniques to recruit unsuspecting individuals to launder illicitly obtained funds in order to conceal the identity, source and

destination.” Agari researchers specifically see Scattered Canary funneling unemployment and CARES payments through prepaid debit cards that let you buy a prepaid card, set it up as a personalized bank account with your name, and then accept your direct deposits, like those issued by unemployment departments and the IRS.

All sorts of hackers are on the prowl amidst the COVID-19 pandemic, deploying ransomware, conducting espionage operations, or scrambling to maintain an edge on public health and treatment measures for the virus. But as millions of people around the world face economic ruin, now is an especially cruel moment to target government programs designed to help them.

This story originally appeared on wired.com.

https://arstechnica.com/?p=1678379