COVID-19 Unemployment Fraud

Author: Darby Wise

Executive Summary

On 21 May, Agari Data published an article highlighting recent Coronavirus (COVID-19)-related unemployment fraud activities victimizing several states across the U.S. and targeting Washington State in particular. Some, if not all, of the threat actors in this campaign belong to Scattered Canary, a Nigerian cybercriminal group behind a variety of fraud campaigns such as social security fraud and tax fraud. In late April, Scattered Canary actors also reportedly submitted fraudulent claims for the CARES Act Economic Impact payments, which were intended to provide funds for families struggling with the effects of the COVID-19 pandemic.[1,2]

The final section of this advisory includes important recommendations for individuals to prevent becoming victimized by these types of activities.

Analysis

Threat actors utilized Gmail "dot accounts" to scale campaign operations. "Dot accounts" refer to a feature built into Gmail accounts that recognizes any variation of an email address with added periods as one singular address, i.e. *googleaccount[@]gmail.com* would be considered the same as *g.o.o.g.l.e.account[@]gmail.com*. These can be used to mass-create accounts for submission to services such as government relief programs, because unlike Google, the websites for these programs recognize the accounts as separate, despite all communications being directed to a single account.[3]

To submit a successful claim, threat actors create fraudulent accounts using stolen personal data such as an individual's name, date of birth, address, and social security number. Agari found that at least 174 fraudulent unemployment claims had been submitted in the state of Washington, and at least 17 in Massachusetts. Agari also reported that 82 fraudulent claims submitted for the CARES Act Economic Impact payments, although it did not provide the targeted locations.

Threat actors used Green Dot cards to collect the money from their fraudulent claims. Green Dot cards are a form of prepaid debit cards that can receive direct deposit payments such as those distributed by government relief programs. Agari found that the threat actors had registered all of the Green Dot accounts under the names of the individuals whose information they had stolen to create and submit the fraudulent unemployment claim.

Prevention and Mitigation

The Employment Security Department of Washington State recommends following the practices below to prevent becoming victimized by unemployment fraud attacks.[4] Individuals there can also visit the official unemployment website at *https://esd.wa.gov/unemployment* to register and verify a real account using a legitimate personal email address to prevent threat actors from being able to create a fraudulent one.

- Be wary of potentially fake or spoofed websites. Use only the official website for each state's employment department; for example, in Washington State: *esd.wa.gov*.
- Be aware that the official website for the employment department will not ask for a payment to process unemployment requests.
- Do not give out personal information over the phone or online other than through a secure eServices account on the official website for unemployment benefits.
- Immediately file a report with the state's employment department if there is a suspicion that someone has applied for unemployment using stolen personal information.

Endnotes

1. https://www.agari.com/email-security-blog/covid-19-unemployment-fraud-cares-act/?utm_source=press-release &utm_medium=prnewswire&utm_campaign=scattered20
2. https://www.agari.com/email-security-blog/scattered-canary-evolves-bec-enterprise/
3. https://www.agari.com/email-security-blog/bec-actors-exploit-google-dot-feature/
4. https://esd.wa.gov/unemployment/unemployment-benefits-fraud

Infoblox
NEXT LEVEL NETWORKING

Infoblox enables next-level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com