SNAPSHOT

THE MEDIA TRUST
We know digital security.

Digital Trends: August 2020

Celebrity scam ads get bolder, contributing to regulatory compliance challenges around the world.

Key Learnings

- Continued increase and evolution of fraudulent scams expose publishers to potential data protection violations and significant financial loss to consumers
- Recommendations:
  - Review campaigns from several different geographic, device, and browser profiles to thwart evasion techniques by emulating real world behavior
  - Analyze landing pages for scam content
  - Continuously update blocking criteria with creative, tag and landing pages confirmed to be propagating the attack

In late 2018, clickbait scams evolved to encompass more sinister elements and cause consumers harm via financial losses and misinformation propagation. The ubiquitous “get rich quick” and “belly fat” ads gave way to scams using celebrity images (many doctored) to promote fake bitcoin investment opportunities, leading many regulatory authorities to issue consumer-directed warnings in summer 2019.

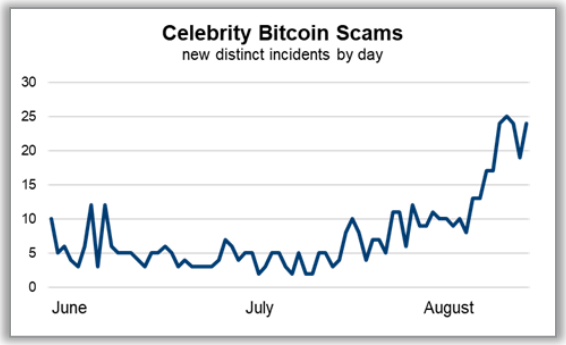

Figure 1: Increase in Celebrity Bitcoin Scams since June

The schemes (sometimes called “Fizzcore”) continue to grow in 2020, now affecting publishers all over the world—on every continent except Antarctica—resulting in a 2.5X increase in August compared to previous months. [Figure 1] Recently, these celebrity bitcoin scams are using more text-based assets to further elude detection. [Figure 2]

Figure 2: Example of more text-based creative driving to compromised landing pages

The Media Trust initially classified these scams as “clickbait” because the creative initiated the first step in the multi-stage campaign. Steadily growing to constitute more than 40% of our clickbait category, the schemes were upgraded to a more severe malware classification due to the increasing volume and reach of these attacks throughout 2020.

One attack, multiple steps, difficult to stop

Celebrity bitcoin attacks take clickbait schemes two steps further beyond the creative by adding landing page and phone call elements. First, these attacks use a celebrity-oriented creative with provocative language encouraging the reader to learn more. As the creative looks like legitimate content it easily passes through basic spam filters and quality reviews. Depending on the user's profile, the landing page is either a fake story wrapped in the publisher's masthead or a bitcoin scam. If clicked, the landing page features a detailed bitcoin investment opportunity, with many containing manufactured celebrity quotes and fake testimonials from supposed investment participants. [Figure 3]

Figure 1: Example of creative and bitcoin scam landing pages

In some instances, visitors are encouraged to participate by providing personal information which is then used by the scammers to contact the user and make a hard sales pitch, thereby executing the final stage of the scam. Not surprisingly, these "investments" are not realized, and the individual is left with no course of recompense.

The campaigns serve different landing pages depending on geography, and these continuously changing landing pages need to be added to blocking appliances, a challenge for those lacking 24/7 support and extensive digital security expertise. In fact, several campaigns in August were detected on publisher sites confirmed to be using malware blocking code, but the landing page behind the ad was not analyzed to detect the scam.

Regulatory Compliance is a global problem

The tightening regulatory environment is cause for publisher concern when it comes to identifying and managing user data collection via their digital properties. Clearly, celebrity bitcoin schemes straddle the data protection line. While voluntarily submitted, user data is being used for unexpected purposes that cause financial harm.

Celebrity bitcoin schemes are regularly seen around the world, with the user's geographic location triggering the malicious activity. The actors frequently use the same text and only update the country in the article and malicious landing page headings. [Figure 4]

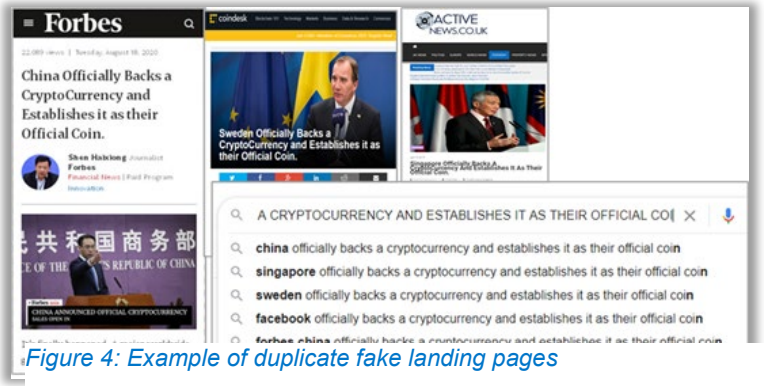

Figure 4: Example of duplicate fake landing pages

This geographic targeting presents a specific problem to media publishers in Europe, which has a stricter regulatory environment due to GDPR. Not only is there more scrutiny of content and misleading advertising campaigns but also local laws favor celebrities when it comes to privacy rights and defamation attacks. For these reasons, executives are more concerned about these attacks than they are about malvertising in general.

Defending against successful attacks

The continued success of celebrity bitcoin attacks rests on their appeal; the desire to learn about celebrities and their lifestyles lures victims to engage. Due to continually evolving evasion techniques, publishers and platforms find it difficult to defend against these attacks.

Adopting the following strategies will help minimize the attacks and avoid the ensuing data protection violations, revenue loss and brand damage:

- **Landing Page reviews**: Pre-flight review of ad tags should include click through to landing pages to verify the authenticity of the content.
- **Ad Quality policy update**: Evaluate your current policy regarding the treatment of clickbait ads to ensure it addresses celebrity bitcoin scams.
- **Digital security expertise:** A proactive team of 24/7 dedicated security analysts need to constantly evaluate new creatives, domains, and tags for malicious activity.
- **Geographic profile scanning**: Execute client-side scans from continuously changing geographic locations to ensure creative, tags and landing pages are clean.
- **Data collection or tracking policy update:** Formalize and communicate expectations regarding unauthorized data collection to your partners. Log vendor acceptance to help demonstrate reasonable care of data protection rights.