SNAPSHOT

THE MEDIA TRUST
We know digital security.

Digital Trends: November 2020

As Bitcoin approaches $20,000, Bitcoin-related malvertising schemes follow suit

Key Learnings

- Strong, positive correlation (0.90) between Bitcoin value and cryptocurrency-driven malvertising
- 7X increase in celebrity Bitcoin incidents since April; a recent 39% increase affects European users
- Recommendations
  - Counteract cloaking techniques by executing client-side scans from various geographic locations to ensure creative, tags and landing pages are clean
  - Analyze landing pages by clicking through creative to capture the true landing page presented to users
  - Update block lists with emerging scam campaign criteria including creatives and tags associated with the scams

Bitcoin, the first and most widely known cryptocurrency, first hit a record high of $19,500 in November after months of steady growth. During this April to November period, The Media Trust detected a corresponding 7X increase in Bitcoin-related malvertising. A closer look reveals a strong, positive correlation of 0.90; as Bitcoin value increases so do Bitcoin-related malvertising incidents. [Figure 1]

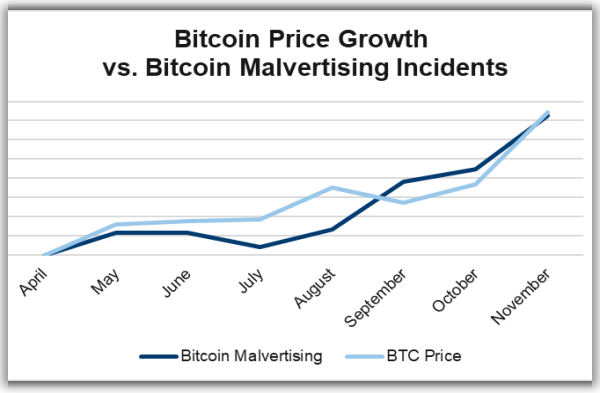

Figure 1: Comparison of Bitcoin value and number of Bitcoin-related malvertising incidents

Primarily affecting Europe-based users, these malvertising incidents use Bitcoin as a form of payment.

Creative or Landing Page cloaking to evade detection

Typically, Bitcoin schemes manifest as clickbait in the digital advertising ecosystem. Bad actors use celebrity-enticing creatives to encourage click throughs to landing pages featuring dubious Bitcoin investment opportunities. Excessive use of cloaking driven by geolocation, device type, and other user-centric variables to present different landing pages (one malicious, one legitimate) helps evade detection. This type of malvertising is a growing lobal problem; November reveals a 59% increase, of which 39% of that growth affects European users. [Figure 2]

Figure 2: Sample creatives and associated landing pages targeting European users in November

Initially, these activities were basic clickbait, but they took a more malicious turn earlier this year by exhibiting more elaborate, multistep scams. The behavior changed again during the past few months. No longer just relying on celebrities to pull in clicks, bad actors have broadened their tactics to include “get rich quick” and “I got a new Ferrari doing this one simple thing” messaging, a reflection of today’s challenging economic environment.

Cryptocurrency is a convenient payment channel

Fueling a crime wave in the past few years, cryptocurrency is at the center of several brazen attacks including ransomware (now an astronomical $6T industry) and the defacement of the Trump campaign website one week before the national US elections. [Figure 3]

Cryptocurrency is a convenient payment method because it is liquid, offers 24/7 trading and is easy to transfer across borders. In addition, it is not centrally managed by a financial institution or government, which makes cryptocurrency more enticing to use—anonymity makes it easier to hide bad intentions.

Figure 3: Screenshot of Trump campaign website when it was hacked for 30 minutes on October 27. The bad actors demanded cryptocurrency in exchange for not releasing damaging information about the president and his family.

Defense against Bitcoin-related scams

With users continuing to experience Bitcoin-related scams, publishers and their AdTech partners need to take steps to minimize the impact of these scams.

AdTech

- 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
- Geographic profile scanning: To counteract cloaking techniques, execute client-side scans from continuously changing geographic locations to ensure creatives, tags and landing pages are clean.
- Digital security expertise: A proactive team of 24/7 dedicated security analysts need to constantly evaluate new creatives, domains, and tags for malicious activity

Publisher

- Geographic profile scanning: To counteract cloaking techniques, execute client-side scans from continuously changing geographic locations to ensure creatives, tags and landing pages are clean.
- Client-side blocking: Use real-time scanning results to update block lists with emerging scams associated with creatives and tag code.
- 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.