SNAPSHOT

THE MEDIA TRUST
We know digital security.

Digital Trends: December 2020

Publishers' embrace of subscription and commerce revenue leaves them vulnerable to disparate malvertising strategies

Key Learnings

- Pandemic ad-spend slowdown accelerates publisher revenue diversification, most notably 3X growth in subscriptions
- 3.5X increase in credit-card-compromising malvertising in 2020, exposing publishers to new attack vectors
- Recommendations
    - Publisher ad ops teams need to align with departments leading payment efforts to mitigate risk.
    - Customer-journey scanning to detect anomalies and emerging threats—particularly of payment pages, where sensitive data is most at risk.

Publishers have been exploring digital revenue diversification outside of advertising for many years, but the pandemic ad-spend slowdown starting in March 2020 put these efforts into overdrive. Affiliate and commerce initiatives have been ramping up, but the most successful burgeoning revenue stream appears to be subscriptions, with the Zuora Subscription Economy Index reporting a 300% growth in digital news and media subscriptions during 2020.

Subscriptions open the door to new threats

Program flexibility and simple implementation make subscription programs attractive to publishers facing ad-revenue struggles, but taking direct payments from consumers leaves publishers (and their users) vulnerable to new malware strategies.

Credit-card compromise schemes affected dozens of publishers and AdTech partners throughout 2020. [Figure 1]

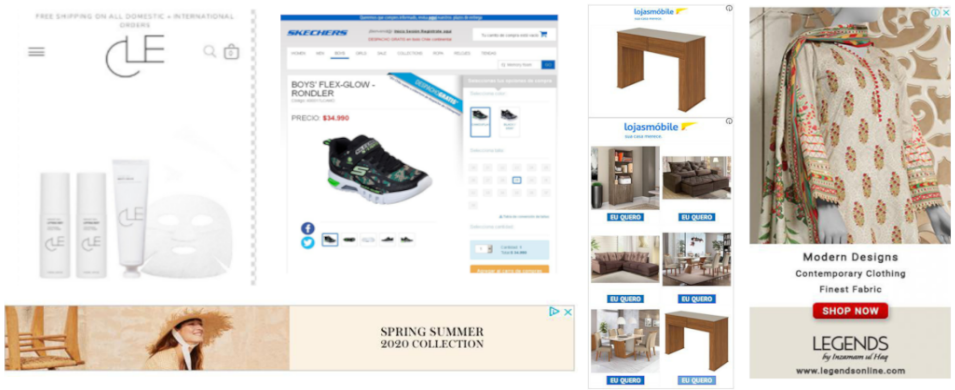

Figure 1: Some of the credit-card compromise creative The Media Trust identified in 2020

Skimming credit card data presents new risks

The most well-known scheme in this area is Magecart—malicious JavaScript skims credit-card information from a payment page. Originally targeting open source Magento CMS but quickly becoming a synecdoche for payment page malware, Magecart schemes can be particularly insidious because hackers will set up multi-pronged attacks and even delay execution of the skimming to avoid detection.

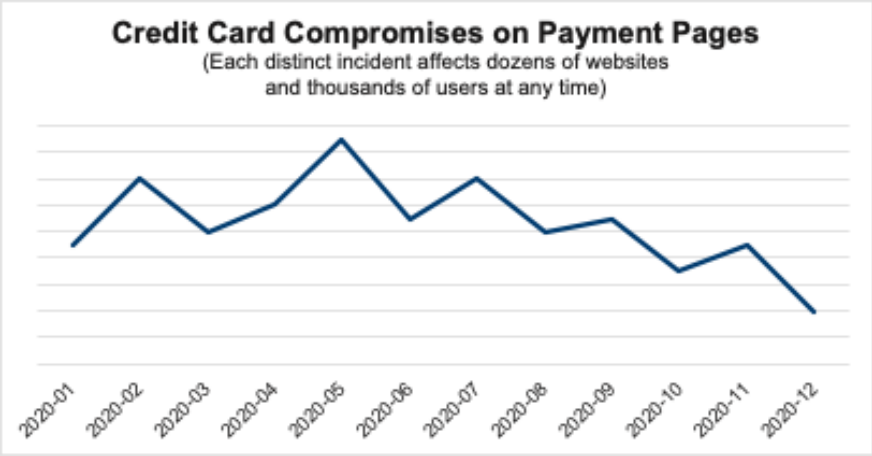

Figure 3: Magecart's alarming spring spike

Credit card stealing schemes aren't new to publishers, as Forbes experienced in 2018. The push for subscription revenue also drove a 350% surge in related attacks in 2020 compared to 2019. [Figure 2]

A May spike can be attributed to an attack targeting AdTech providers and a few mid-tier publishers. As brands upped their security prerogatives and took more time in launching campaigns, the scheme proved less ubiquitous later in the year. However, scammers—and especially deployers of Magecart—are cyclical creatures, taking their time and testing till they're confident about a scheme.

New hunting grounds?

Publishers embracing subscription products as well as commerce programs that enable direct payments from consumers greatly enlarges the realm of targets for Magecart. Another wrinkle: subscription and commerce programs tend to be managed by departments separate or adjacent from the ad operations folks on the hunt for malvertising, and the payment processing services are typically provided by third parties.

These are gaps that bad actors can and will take advantage of—diligence requires some extra steps. It's essential that you align with the departments running direct-payment programs so they're aware of scams like Magecart and how the payload is delivered.

Recommendations

- Examine and monitor the entire customer journey. Apply controlled scanning to the offer, checkout, payment, and confirmation pages. All four of these can offer interesting data—for example, what cookies are popping up on the payment pages? What is *this* vendor doing here?
- Ensure all third-party code running on your site is coming from authorized vendors on your inclusion list.
- Now more than ever you should be scanning all creative assets and pages where payments are accepted for anomalous, emerging threats.
- And never, ever stop blocking known malware.