Timeline of a Malvertising Attack

How malicious ads go from idea to threat and how HUMAN Malvertising Defense helps publishers protect their valuable revenue from this ever-evolving threat.

1. Bad actor creates malicious code and sets up a programmatic ad campaign

2. Pre-scanning tools check for malicious activity in creative, but malvertiser evades blocklist detection

3. Creative renders and malvertiser pays for impressions

4. Code begins to execute malicious activity

5. Malicious code affects users and damages publisher revenue

6. Malvertising threats for Publishers

   - Redirects away from publisher sites
   - Ad cloaking to execute clickbait scams
   - Redirects to malicious landing pages
   - Client-side injections to steal user info
   - Distribution of malware
   - Heavy ads slowing site experience
   - Pixel/Video Stuffing

7. Without HUMAN

   - Blocklists try to catch known bad actors, but malvertiser evades blocklist detection
   - Non-malicious ads can get blocked, causing unwanted revenue loss
   - Add Latency
     - Size of the blocklist can cause latency on pages due to list load
   - Easy to Evade
     - Blocklists are reactive and only as good as the entries within them.
   - Put Revenue at risk
     - Blocking ads and requesting new creative can risk revenue or diminish user experience

8. Protected by HUMAN Malvertising Defense

   - Malvertising Defense scans all creatives on page and analyzes landing pages to detect malicious behavior
   - Creative renders, but malicious behavior is blocked
   - User experience is unaffected, publisher revenue is protected and malvertiser will look elsewhere for future attacks

Malvertising Defense Advantage

- Preserve Revenue
- Protect Brand Reputation
- Optimize Performance and Overhead

Take Control of Your Digital Ad Inventory

Find out how HUMAN uses modern defense strategies to help publishers safeguard their users and revenue from malicious ads. Visit HUMAN to request a demo.