SNAPSHOT

THE MEDIA TRUST
We know digital security.

Digital Trends: September 2020

Malware on landing pages is on the rise, highlighting the need for comprehensive ad quality across the digital supply chain, from brands/agencies to adtech to publishers.

Key Insights

- Malware exclusively found on click-through landing pages almost doubles in the past two quarters
- Ad quality conscious industry players are increasingly blocking campaigns with malicious landing pages
- Recommendations:
  - Expand ad quality reviews to include landing page malware checks
  - Evaluate landing pages via Creative Click Through, Landing Page URL, or Bid Response
  - Execute continuous scanning to catch landing page switches post campaign go-live date

The ultimate goal of any campaign is for an advertiser's creative to result in a consumer clicking on an ad that takes them to the advertiser's landing page. Since March of this year, landing pages have become an important vector for malware. What was once a small amount is now on nearly 1 in every 5 incidents detected, signaling a pivot in malvertising tactics.

Malvertising Vector: Landing Pages

Advertising campaigns contain three elements—creative, tag code (JS, HTML, etc.) and landing page—and each of those elements can be compromised. This is why TAG's Certified Against Malware program requires scanning of each element. However, most commercial blockers don't address landing pages. The result is an escalation in malware that only affects landing pages; the malware is not present in creative or tags.

Landing pages are a great place to hide malicious code. Bad actors leverage the power of a legitimate advertising campaign to bypass malware blockers, access an engaged audience, and expose those visitors to malware. This malicious activity comes in many forms, ranging from the seemingly benign unwanted toolbars to the more serious redirects, ad fraud, and bot propagation.

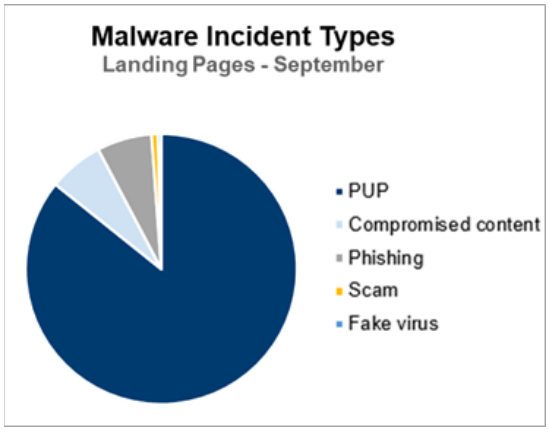

Figure 1: Malware types found on landing pages

Even more interesting than this doubling of malware only affecting the landing page is the composition of the malicious incident types. [Figure 1] The majority of this "creative click" landing page malware comes in the form of potentially unwanted programs (PUP) such as knock-off PDF readers, toolbars, or cheap browser games. While frequently classified as harmless but possibly annoying adware, more security researchers are realizing, adware is a conduit for full-blown malicious activity.

Further analysis of malicious landing pages reveals that 80% are due to compromised third-party page tools and 20% are from owned & operated code. In other words, most of the malware found on landing pages can be attributed to unmanaged third-party code provided by digital partners.

Enabling consumer-harming activity and disrupting revenue

Landing page malware is an increasing source of hard-to-rectify user complaints, including exposure to consumer fraud scenarios. In more than one instance publishers have been plagued with porn on the page that did not originate through their ad server; it came from other third-party vendors used in the landing page's build. And, let's not forget that landing pages enabling credit card theft (Magecart), celebrity bitcoin scams (FizzCore), and Coronavirus scams still continue to haunt the digital ecosystem, affecting millions of consumers each month.

While publishers tend to use tools that block at the ad level, many SSPs block the entire domain. As the advertiser's landing page is typically leading to their main website, this action blocks the advertiser and renders their advertising campaigns ineffective. More often than not, a DSP is surprised to learn that a reliable partner—often an eCommerce brand—has been blocked, but upon investigation they are shown that the landing page—not the creative or tag—contains the malicious content.

Pushing Ad Quality concerns upstream

Each participant in the digital advertising supply chain is responsible for the quality of the content trafficked and/or served to users. However, the groups have different incentives:

- Publishers: Bear the brunt of complaints because they are closest to end users.
- SSP: To maintain access to inventory, SSPs need to protect their publisher relationships.
- DSP: As groups of client campaigns can be blocked, they experience a noticeable revenue impact.
- Agency/Advertiser: Closest to the advertiser, agency campaign work will not yield the expected returns. In addition, they often build campaign-specific landing pages that are forgotten and/or parked; these pages are often compromised or purchased by bad actors.

Avoid digital supply chain disruption by evaluating landing pages including both pre-and in-flight campaigns. Landing page evaluation is accomplished by one of these methods:

- **Continuous Scanning:** A "one and done" approach to scanning is inadequate. Continuous, client-side monitoring from a variety of user profiles will catch landing page changes.
- **Creative Click Through:** Execute a click on the creative to capture the redirect action and the landing page content. For adtech this is accomplished via an API to click through on tags.
- **Landing Page URL Scanning:** Ask your upstream client for the landing page asset URL. Scan the entire page, not just a particular domain
- **Bid Response Extraction:** Usually available to adtech providers, the ADMA (ad markup and/or link shortener) can be accessed to extract the landing page from bid response