TAG INDUSTRY BRIEF:

Increasing Brand Safety Through Malware Scanning

A recent survey of U.S. consumers conducted by the Brand Safety Institute (BSI) and the Trustworthy Accountability Group (TAG) found that 93% of respondents would reduce their spending on an advertised product if the ad had infected their computers or mobile devices with malware, and 73% would stop buying that product altogether. These findings highlight the significant financial risk that brands face if their ads are found to be "malvertising," carrying malware payloads that can harm the very consumers their ad campaigns seek to engage.

Since 2016, TAG's Certified Against Malware Program has provided companies with a playbook by which to combat malvertising across the digital advertising supply chain – including the regular scanning of campaign assets and associated landing page click-thru URLs to detect and remove malware. Marketers that are serious about brand safety should work with trusted partners, including those who are Certified Against Malware.

In order to achieve TAG's Certified Against Malware Seal, companies must scan a reasonable percentage of campaign assets and landing pages for malicious activity or payloads prior to a campaign being launched. Further, companies must disclose to TAG their malware scanning methodology and the percentage of such assets scanned prior to launch. While it may not be necessary to perform an initial scan when campaign assets are received from a trusted partner, rescanning is vital because the greatest threat of malware occurs after a campaign has gone live, when criminals are well-known for updating and swapping-out campaign assets after the initial approval process. Therefore, certifying companies are also required to diligently rescan 100% of those assets and landing pages throughout the life of a campaign, disclosing to TAG the frequency at which those rescans occur and the vendors or technologies used to execute those scans.

Key Takeaways

In a review of all companies recertifying their Certified Against Malware seal in 2019, as well as those companies who have earned the Certified Against Malware seal during the course of this year, TAG found that:

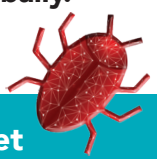
100% **of certified companies commit to scanning a reasonable percentage of campaign assets and landing pages** they handle before a campaign launches, as a requirement of the program.

In addition:

83% **of certified companies perform initial malware scans on all of the campaign assets and landing pages** they handle before launch.

92% **of the campaign assets and landing pages** handled by certified companies handle were scanned prior to initial delivery, on average.

76% **of Certified Against Malware companies apply these best practices globally.**



Even more impressive are the lengths to which Even more impressive are the lengths to which certified companies go to in order to ensure that campaign assets and landing pages remain free of malware payloads once a campaign goes live.

100% of certified companies commit to rescanning all of campaign assets and landing pages on a reasonable frequency, as a requirement of the program.

Some follow a daily methodology – rescanning 100% of campaign assets and landing page each and every day. Others have developed risk-based or volume-based methodologies to ensure that assets presenting the greatest risk are rescanned at the greatest frequency.

50% of certified companies employ a daily rescan methodology, rescanning every campaign asset and landing page at least once daily. Some companies perform rescans as frequently as every 15-30 minutes.

25% of certified companies use a risk-based rescan methodology, performing risk assessments for each of their partners and placing them into a risk tiers to determine how frequently particular campaign assets and landing pages should be rescanned. Assets from newer and potentiality risker partners are scanned more frequently than those associated with longer-term, well- established partnerships. Assets from partners in the highest risk tier are rescanned daily, at a minimum, while those of partners in lower risk tiers may be rescanned every 2-7 days.

25% of certified companies follow a volume-based rescan methodology, organizing campaigns into ad-volume tiers which determine rescan rates. High-volume ads may be rescanned daily or multiple-times-per-day, while lower volume ads are scanned less frequently.

The scanning best practices of Certified Against Malware companies offer an important baseline for any brand serious about keeping its ads from being associated with malvertising. TAG will strengthen the Certified Against Malware Program even further by reflecting these best practices in future program requirements.

As highlighted in the consumer research by TAG and BSI, there is a growing awareness among comsumers about malware threats. The digital advertising indsutry has reacted with greater vigilance and strengthened anti-malware practices, including increased participation in the TAG's Certified Against Malware Program. In 2019 alone, the program has grown by more than 33%, reflecting the reality that the Certified Against Malware Seal is increasingly a primary way that responsible companies communicate their commitment to protecting consumers and their clients.