Global media company improves malware detection and remediation times

Every day ad networks and exchanges move millions of advertisements across the online and mobile advertising ecosystem, providing malware purveyors countless opportunities to launch ad-based malware attacks. Information security and ad operations professionals at a global media company wanted to significantly reduce their malware exposure on their company's websites. However, like many digital publishers, they lacked the internal tools and resources to easily identify which of the thousands of ads served to their sites may have been injected with malicious code.

Continuous, 24/7 monitoring of ad tags

Starting in 2011, the company's Ad Operations team remedied their lack of internal tools by partnering with The Media Trust. With its proprietary website and ad tag scanning technology, The Media Trust protects websites, mobile apps and ad tags from web-based malware, unwanted third-party code and data leakage of first-party data, all of which lead to lost revenue and privacy concerns.

The Ad Operations team employed The Media Trust's Media Scanner for Ad Tags service to scan—on a continuous, 24/7 basis—every ad tag served to the company's websites. This SaaS-based service receives the tags from the company's ad serving systems via APIs and immediately begins scanning for suspicious or malicious behavior. The Media Scanner service provides two types of scanning:

- Pre-scan: a thorough scan of all ad tags and creatives prior to launch
- Live-scan: Ongoing scanning of ad tags and creatives throughout the campaign flight

Both types of scanning use geographies defined by the Ad Operations team as well as multiple browser, OS,

SUMMARY

- Industry: Digital publishing

- Challenge: Compressing cycle times for malware detection and remediation

- Solutions:
  - Media Scanner for Ad Tags
  - Media Scanner for Websites
  - Media Scanner for Resolution Services

- End User: Ad Operations; IT/Security Team

- Results:
  - Achieved malware detection accuracy rate of 99.95%
  - Compressed malware remediation time from 48 to 4 hours
  - Strengthened security posture via real-time information sharing
  - Optimized revenue streams by ensuring ad tags are always 100% active

> " The improvements we gained from Media Scanner for Ad Tags were significant, and the ROI realized from Media Scanner for Resolution Services quickly exceeded our expectations. "

Media Scanner for Ad Tags detects infected ad tags in real time
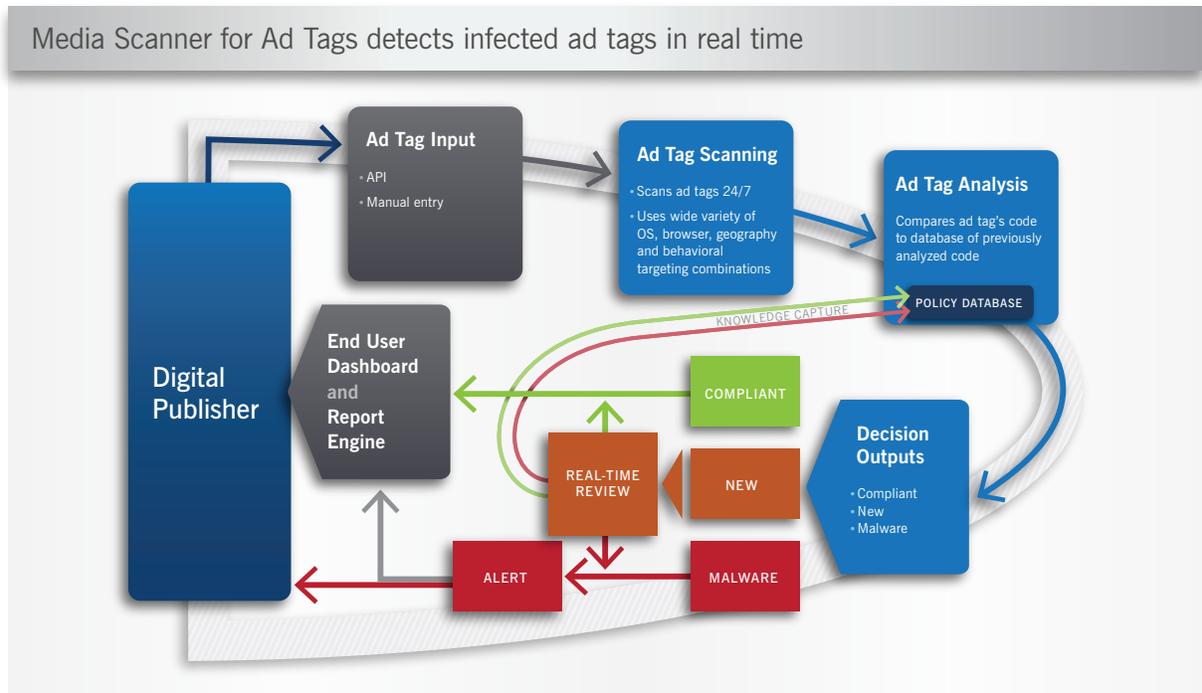
Media Scanner for Ad Tags has provided the global media company with real-time malvertising detection and alerting that is more than 99.95% accurate since 2011.

device-type and behavioral targeting combinations. Upon detection of any anomalies or malvertising, the service immediately notifies the Advertising Operations and Technology Security teams so they can block the offending tag, significantly reducing the malicious code's ability to inflict harm. In the unlikely event that the malicious activity persists, The Media Trust's Malware Team works with the Ad Operations and Technology Security teams to determine appropriate next steps.

The Media Trust Malware Team also captures and isolates the suspect code and begins a forensic examination to determine its intent, purpose, pathway and origin. This in-depth analysis not only enables quick resolution for the global media company, but further develops The Media Trust's institutional knowledge of malware.

Since 2011, Media Scanner for Ad Tags has provided the global media company with a malvertising detection accuracy rate of more than 99.95%, enabling the Ad Operations team to significantly compress their cycle time for malware detection and remediation, reduce their labor costs and improve their service levels.

In the unlikely event that malware actually infiltrates a site, The Media Trust provides crucial support during the remediation process. Given each site's substantial size, trying to manually identify the malware's location and understand how it works would be extremely difficult and time consuming. In comparison, Media Scanner's proprietary technology actually observes and captures— in real time—how and where the malware is propagating, providing Ad Operations with the affected domain name,

a copy of the tag's source code executing on the site and critical information about the malware's delivery mechanism. With this real-time attack information, the company can quickly locate, remediate and mitigate the attack, saving significant time and revenue.
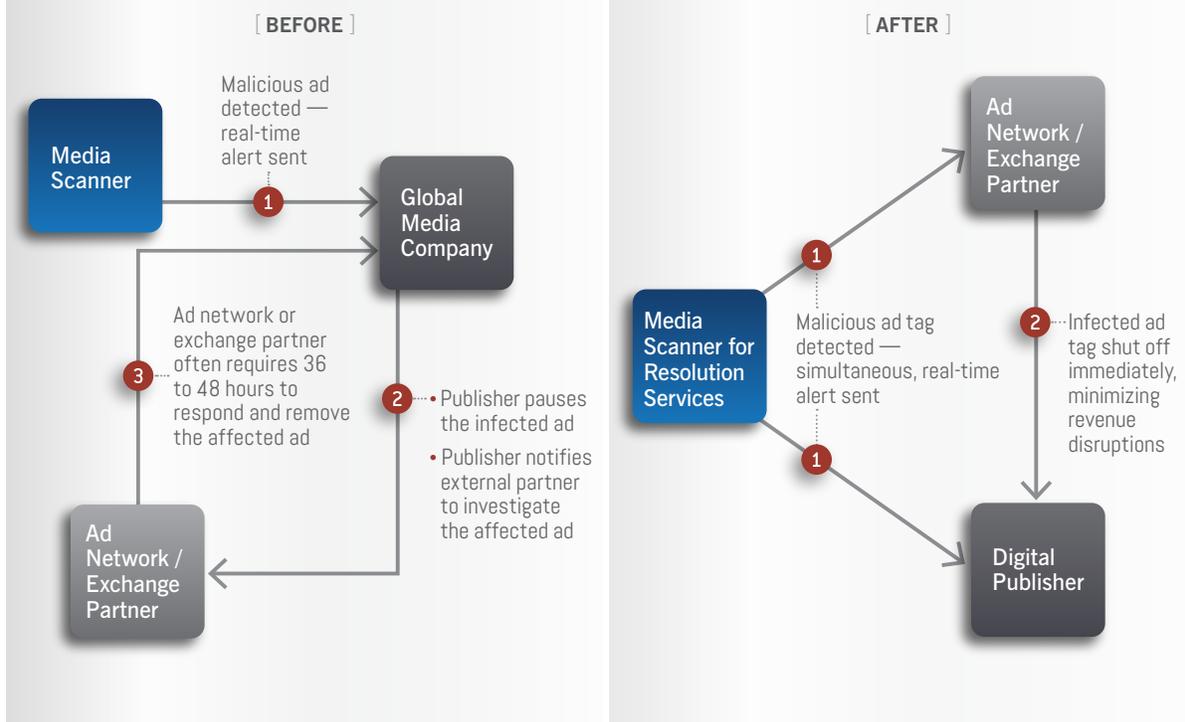
Leveraging real-time malware information sharing

The Media Trust determined an additional reduction in remediation time was possible if digital publishers were willing to share malware information in real-time with their ad network and exchange partners. Recognizing real-time information sharing could save additional time and money, the global media company agreed to be a beta customer for The Media Trust's new product Media Scanner for Resolution Services.

Previously, when an infected tag was detected, the Ad Operations team immediately paused the affected tag and sent an email to the relevant ad network or exchange partner to request an investigation. The partner often took 36 to 48 hours to respond during which time the affected tag remained paused and unable to generate revenue. Now, when Media Scanner for Ad Tags detects a malicious ad tag and instantly notifies the Ad Operations and Technology Security teams, Media Scanner for Resolution Services simultaneously sends the same alert to the ad network and exchange partner(s) involved in serving of the malicious tag.

"The initial improvement we gained from using Media Scanner for Ad Tags was significant; however our cycle times for remediation were still too long," says the director of the media company's Technology Security team.

Media Scanner for Resolution Services decreases malware remediation times

[**BEFORE**]

Malicious ad detected — real-time alert sent

Media Scanner → **1** → Global Media Company

Ad network or exchange partner often requires 36 to 48 hours to respond and remove the affected ad → **3**

2 • Publisher pauses the infected ad
• Publisher notifies external partner to investigate the affected ad

Ad Network / Exchange Partner

[**AFTER**]

Ad Network / Exchange Partner

Media Scanner for Resolution Services → **1**

Malicious ad tag detected — simultaneous, real-time alert sent

2 Infected ad tag shut off immediately, minimizing revenue disruptions

1

Digital Publisher

With Media Scanner for Resolution Services, the global media company and their ad network and exchange partners simultaneously receive the same real-time alert, compressing the malware remediation process from 48 hours to less than four hours.

"Working with The Media Trust, we realized that immediately sharing threat intelligence with the ad networks and exchanges was the most effective way to further compress cycle times, with the additional reductions generated by Media Scanner for Resolution Services exceeding our expectations. We're thrilled to be an early adopter of this cooperative, intra-industry approach to malvertising remediation."

The alert sent by Resolution Services contains only the information needed to remove and block the specific malicious ad—the vendor, ad tag name, the domain, the pathway and the affected creative—with no other data accessed or sent. The Ad Operations team has complete control over which ad network and exchange partners are included in the Resolution Services program.

Receiving the real-time alert at the same time allows the ad network and exchange partners to also instantly block and remove the offending tag, compressing the remediation process from 48 hours to less than four hours. As a result, the level of protection improved exponentially, while significantly eliminating the labor associated with the Ad Operations team identifying and then notifying the affected ad network and exchange partners. This resultant positive network externality improves not just the health of the media company's own individual ad execution value chain, but also the health of the greater online and mobile advertising ecosystem.

Additional refinements drive additional cost savings

The Ad Operations and Technology Security teams want to further reduce their remediation time. The next step is to share Resolution Services notifications with authorized ad network and exchange partners via an API. With this approach, Media Scanner for Resolution Service will communicate directly with the ad network and exchange partner's systems, which will enable the immediate and automatic removal of the infected ad without any human intervention, further compressing the cycle time from four hours to potentially less than four seconds!

"Resolution Services is a simple and cost-effective solution to a seemingly endless threat vector. We immediately realized the service's benefits, with the ROI more than exceeding our expectations," says the Ad Operation Team's vice president. "The reality is that if every publisher used this service, not only would the health of their own website improve dramatically, but also the health of the entire online and mobile advertising ecosystem."

Citing Media Scanner's malware detection accuracy rate of 99.95%, the global media company informed several ad exchange and network partners that second-source validation was no longer required to turn off infected ads. This validation process often took several days, providing the malicious code ample time to harm site visitors and damage the site's brand reputation.

Conclusion

Malvertising is a fact of life for ad-supported websites, but traditional information security tools cannot protect against these attacks in real-time. While the vast majority of online and mobile ads are completely safe, digital publishers must remain vigilant. The only way to mitigate these threats is though 24/7 monitoring of digital properties. To address these challenges, the global media company uses Media Scanner for Ad Tags, a SaaS-based service that dramatically improved their ability to detect and remediate ad-based malware in real time. Striving for continued improvement, the company became an early adopter of Media Scanner for Resolution Services, which exponentially compressed the remediation process from up to 48 hours to less than four hours.

Together, these two services provide a complete, holistic approach to malvertising detection and remediation, resulting in a streamlined remediation process and a significantly safer browsing experience for website consumers. Another key benefit is the improved communication and cooperation between the digital publisher and their ad network and exchange partners, which severely limits malvertising's reach and success rate and improves the overall health of the entire online and mobile advertising ecosystem.

"The pervasive nature of malvertising requires Information Security teams to extend their protection beyond the firewall and DMZ to where the consumer's browser interacts with the third-party code rendering the site. It's here that infected ad tags operate with little fear of detection," says the media company's CISO. "Media Scanner for Ad Tags and Media Scanner for Resolution Services both extends and strengthens our security posture by providing real-time visibility, control and information sharing on the ad tags served to our site, enabling robust, 24/7 protection of the consumer's browsing experience."

The Media Trust

The Media Trust works with the world's largest, most-heavily trafficked digital properties to provide real-time security, first-party data protection and privacy, performance management and quality assurance solutions that help protect, monetize and optimize the user experience across desktop, smartphone, tablet and gaming devices.

As the global leader in monitoring the digital—online and mobile—ecosystem, The Media Trust leverages a physical presence in 65 countries and 500 cities around the globe to continuously scan websites, ad tags and mobile apps and alert on anomalies affecting websites and visitors alike. More than 500 publishers, ad networks, exchanges, agencies and corporates—including 40 of comScore's AdFocus Top 50 websites—rely on The Media Trust to protect their website, their employee internet use, their revenue and, most importantly, their brand.

The Media Trust
1749 Old Meadow Road
Suite 500
McLean, VA 22102
703.893.0325
www.themediatrust.com
@TheMediaTrust