CYA* 2023

7 Digital Safety Trends for Uncertain Times

Threat actors expand attacks on children and the elderly while diversifying malware deployment strategies to leverage compromised brand websites and URL-sync errors

*Cover Your (Digital) Assets

THE MEDIA TRUST
Digital Safety. Delivered.

EXECUTIVE SUMMARY

"Information is the resolution of uncertainty."
—Claude Shannon, American Mathematician

"The sign of a civilised society is how we treat the most vulnerable."
—Matt Hancock, UK Politician

As 2023 kicks off in earnest, economic headwinds and inflationary pressures have deposited consumers in an ocean of uncertainty. Fittingly, the entire digital ecosystem—especially the advertising engine that fuels it—is reflecting this acute anxiety.

Major platforms have reported declining revenues year over year, and substantial layoffs at large advertising technology (AdTech) and digital publishing companies at the end of 2022 drew much industry consternation. While eMarketer and IAB project digital advertising spend growth—albeit at a lower rate—advertisers are signaling a significant pullback in spend and typically modest first quarter revenue forecasts are looking grim.

Threat actors view this uncertainty as an excellent opportunity to spread malware and sow discord. Data from 2022 confirm they are doubling down on tried-and-true tactics (Figure 1) while discovering new vulnerabilities that widen attack surfaces. This includes compromising websites and apps to turn legit brand assets into malware distribution centers as well as corrupting cookie syncs to drop backdoors and phishing attacks.

Threat actors are increasingly targeting the most vulnerable online—including children and the elderly—and deploying campaigns that prey on technological inexperience. Taking advantage of low programmatic CPMs, straightforward scammers are barely masking their malicious intent.

To further complicate this picture, sensitive, regulated, and potentially brand-unsafe content continues to diversify. A long and brutal political season in the US unleashed all manner of contentious advertising around immigration and abortion. Fallout in the cryptocurrency market raises questions about which advertisers are truly credulous. And as more states and countries append regulations around gambling and marijuana, how do businesses (e.g., retail media, publishers, and platforms) adjust policies to maximize revenue while not offending or alienating consumers?

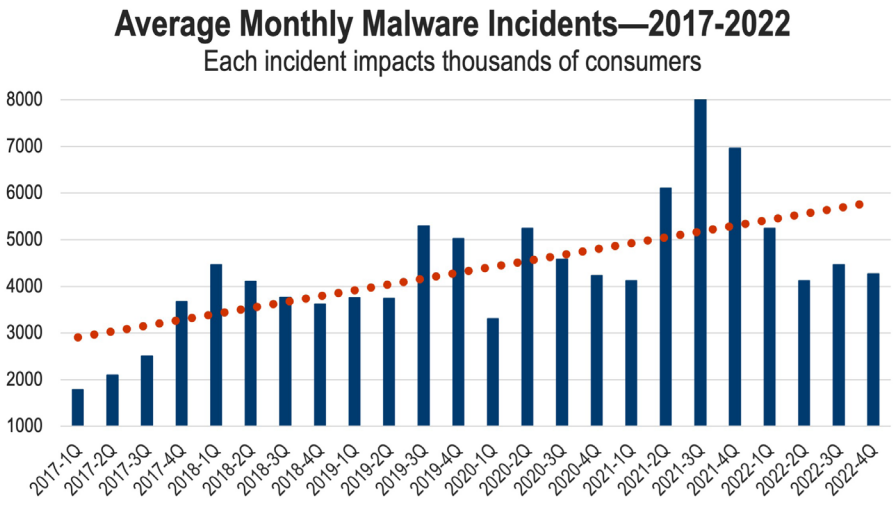

Figure 1: Average monthly malware incidents fell by 28% in 2022 due to threat actors focusing on high-performing attacks and The Media Trust recalibrating its incident classification system to better group threats. Over a 5-year period, malware attacks are up 140%.

With consumers feeling more vulnerable than ever, it is imperative that companies across the connected digital landscape ensure digital trust and safety. Threat actors are flooding digital environments with malicious activity; any cost reductions or revenue gains that come from diminished vigilance will quickly be lost as consumers experience digital harm.

This report illuminates 7 trends in malware and sensitive ad content for 2023 that will aid you in keeping consumers safe and satisfied during a perilous moment. Providing digital trust and safety is crucial for your business' success, especially as uncertainty reigns supreme.

2022 BY THE NUMBERS

Everyday Internet use—news, entertainment, shopping, travel—exposes consumers to unprecedented risk.

4,526	average malware incidents* thwarted monthly
51,020	malicious domains identified and added to blocklist
1.3 billion	malicious ads blocked on Fortune 1000 websites and apps
3.7X	spike in threats targeting children compared to 2021
110%	increase in malicious attacks on elderly consumers
2.2X	growth in e-skimming attacks since 2020
114%	increase in crypto ads blocked in 4Q2022
3X	increase in incidents of named threat MimicManager-3PC since first appearing in Sept. 2022
160%	rise in backdoor malware that leaves businesses and consumers vulnerable to future and more harmful attacks

*Each incident impacts thousands of consumers

What Is Digital Trust and Safety?

Ensuring consumer well-being across the connected digital landscape through governing content- and conduct-related risk. The three central tenets:

SECURITY: Protecting consumers from malware and digital harms

DATA: Safeguarding consumer privacy

CONTENT: Ensuring benign consumption of digital media

Threat Behavior

In 2022 The Media Trust introduced the Threat Behavior label to better illustrate how malware directly harms consumers: 6 streamlined categories with straightforward definitions and clear examples (e.g., ransomware is a type of backdoor).

THREAT	DEFINITION	EXAMPLES
Backdoor	Attacks that deliver a wide variety of known malicious payloads with or without user interaction.	Ransomware, Keylogger, Credential Harvesting, Remote Access Trojan (RAT), DDoS Bot, Cryptominer
Phishing	Auto-redirects to popups and browser hijacks using fake surveys and/or other malicious content seeking sensitive information from consumers.	Data Exfiltration, Cloaking, Exploit Kit, APKs, Ad Injector, DDoS Bot, Credential Harvesting
Scam	Schemes to defraud consumers or mislead them into sharing personal info that can be leveraged in future attacks.	Data Exfiltration, Misinformation, Command & Control Communication, DNS Tunneling
E-skimming	Attacks employing malicious files for theft and/or unauthorized use of consumers' sensitive data.	SQL injection, Credential Harvesting, Arbitrary Code Injection, Cryptojacking, Cross-Site Scripting, Remote-Code Execution
Generic Malware/ Suspicious	Content containing characteristics and previously detected patterns of known malicious attacks and threat actors.	Domain Hijacking, Heuristics attack match
Ad Fraud	Content executing click and/or impression fraud.	Impression Fraud, Click Fraud, Clickjacking, Ad Stuffing, Ad Stacking

1. Attacks on Vulnerable Consumers

Threat actors are increasingly taking aim at the most vulnerable consumers of digital society: children and the elderly. The expectation of safety and/or lack of technological prowess makes these consumer groups more susceptible to orchestrated attacks. Between May and the end of 2022, attacks aimed at children 12 and under increased by 3.7X while malicious campaigns targeting the elderly rose 180% (Figure 2).

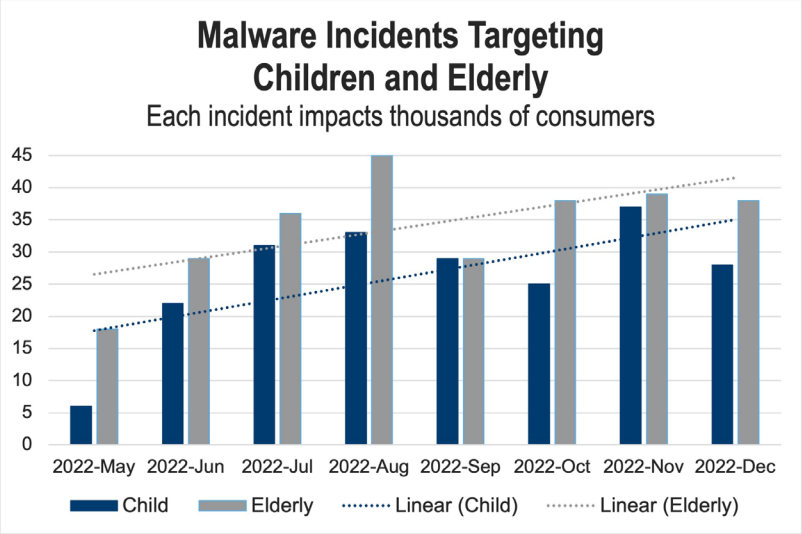

Figure 2: Attacks aimed at children and the elderly ramped up from May to the end of 2022.

Both groups were besieged by two new named threats designed to take advantage of technological inexperience. Dolos-3PC, which has a global potential reach of 1.6 billion consumers, repackaged a classic malware scheme: a pop-up on clickthrough informs a consumer that their Windows device is infected and they need to call a technical support number immediately (Figure 3).

When dialed, the "technical support" operator asks for remote access to the consumer's device and installs backdoor software for future attacks. Potentially this could extend to a consumer's employer, whether it be a business, government office, or military facility.

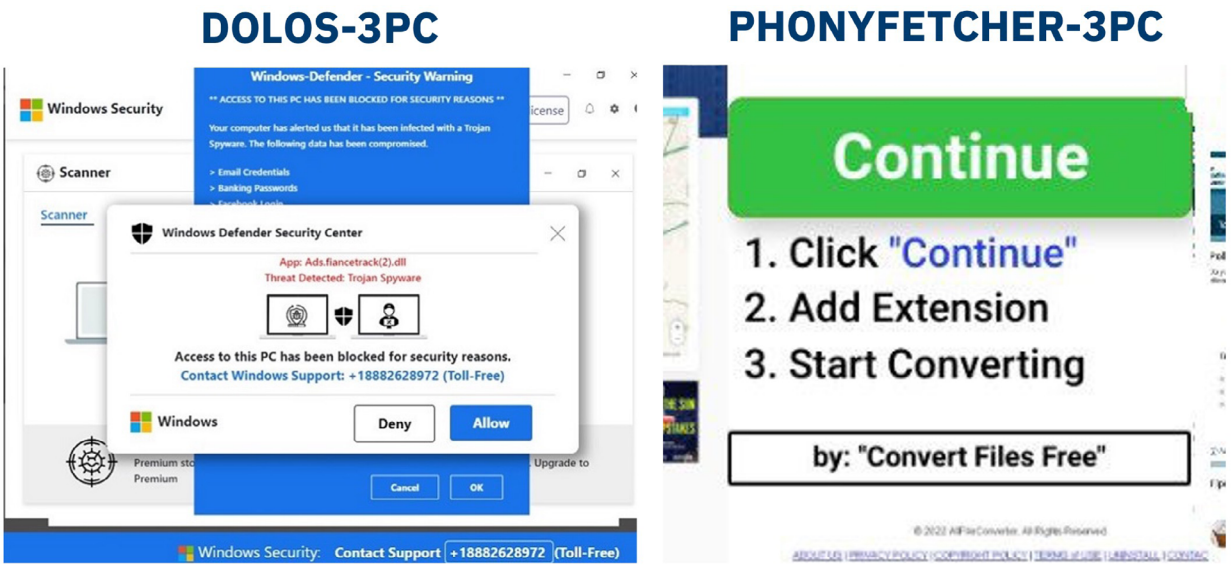

Figure 3: Dolos and PhonyFetcher attacks targeting elderly and children increased 45% between September and end of year.

PhonyFetcher-3PC is also a rehaul of the old-school search toolbar scheme. Ads offer a free document conversion browser extension or other utility service, but once installed, this adware opens the consumer's device to a variety of threats delivered via the advertising supply chain.

DEFENSIVE MANUEVERS

- **Dolos-3PC uses a redirect on consumer click to launch its pop-ups; platforms must scrutinize clickthroughs and campaign landing pages to ensure they are malware-free. In addition, scanning must leverage multiple device profiles as Dolos is targeted**
- **AdTech platforms should consider refusing advertising for any "free" or ad-supported browser extensions, as these typically deliver malware to consumers—intentionally or unintentionally.**
- **As the last line of consumer defense, publishers must employ a creative blocker fueled by the most up-to-date malware data. That requires in-house malware analysis, rather than reliance on third-party sources that tend to be outdated.**

DIGITAL TARGETING AND CYBER SECURITY:

Malware as a War Machine in Ukraine

Russia's invasion of Ukraine unfortunately demonstrated how state actors use digital cyber attacks alongside air and ground offenses. Ukrainian citizens were targeted with phishing and backdoor attacks before and during the war's start to disrupt the country's digital ecosystem (Figure 4). Outbreaks diminished as the conflict raged on during the summer, but ramped up again in September as Ukrainian forces retook occupied territories. Cyberwarfare via targeted advertising has become a critical tool in major conflicts.

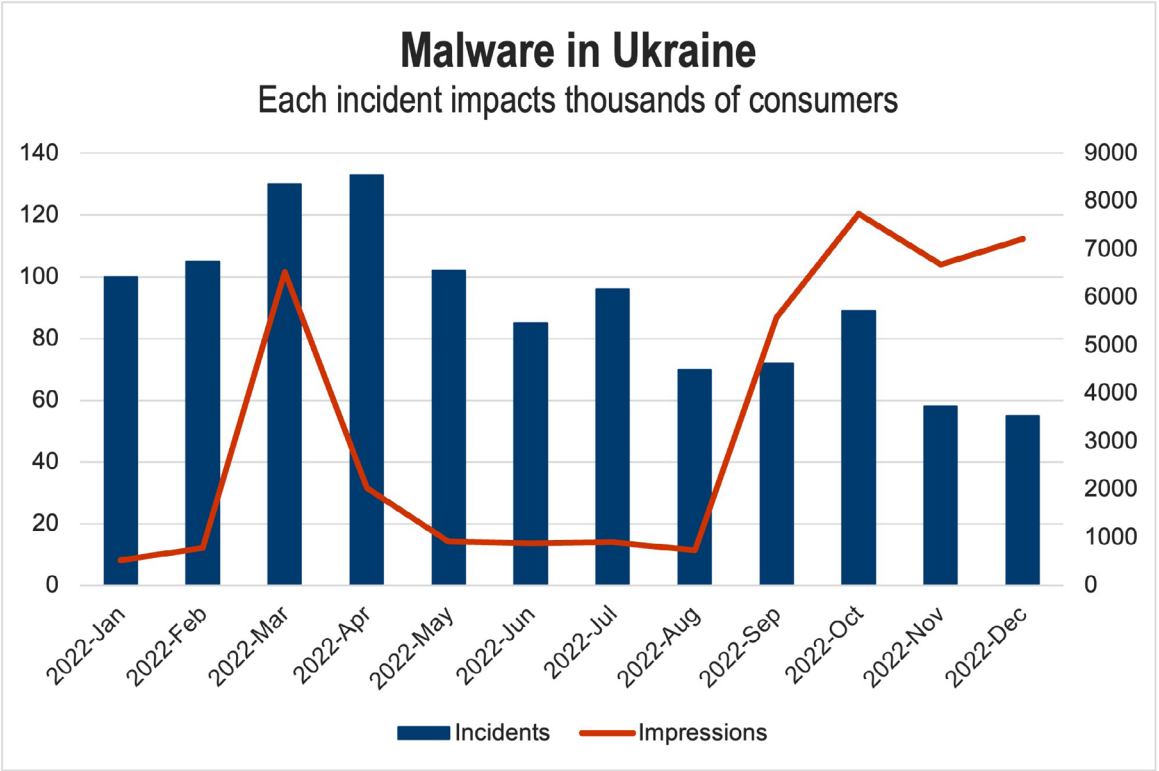

Figure 4: Alongside the territorial invasion, Ukrainian citizens have been terrorized by digital assaults.

2. Reign of GhostCat

Since 2019, mobile-targeting phishing malware GhostCat-3PC has terrorized the digital media ecosystem with at least one major assault every year. A steady presence throughout 2022 with a potential reach of 3 billion consumers, GhostCat exploded in August, with attacks growing 4.1X month over month (Figure 5).

GhostCat serves as a perfect lens to examine the growing sophistication of malvertisers—those that use the digital advertising supply chain as a malware distribution channel. The threat boasts neither a creative or a campaign landing page URL, making it a streamlined malware delivery device. GhostCat also only unleashes its malicious payload if targeting parameters (i.e., consumer using a mobile device) are satisfied, helping it dodge creative audits and execute undetected for long periods of time.

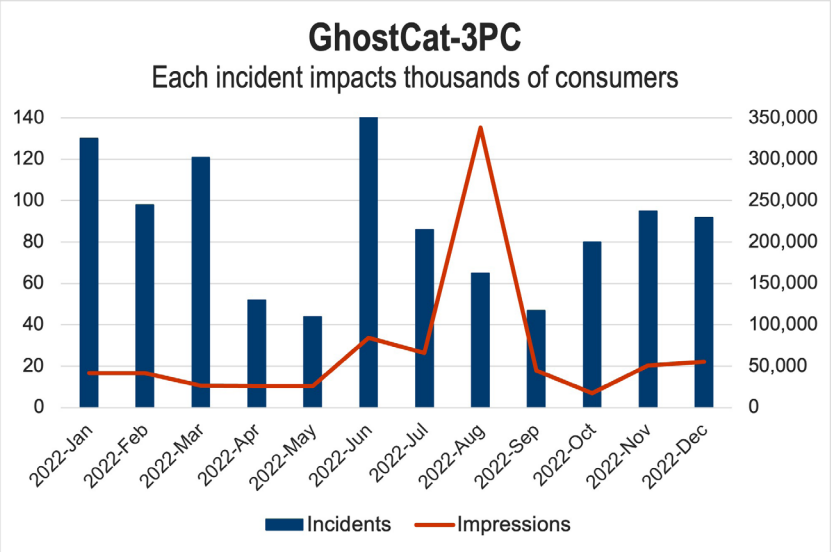

Figure 5: GhostCat incidents were a steady presence throughout 2022, but a consolidated group of incidents accounted for a massive outbreak in August.

GhostCat demonstrates the enhanced threat of advanced malvertisers: rather than bombarding media with redirects, malware propagators deploy calculated, highly targeted attacks to maximize consumer harm. GhostCat's operators engage in long testing periods, probing the broader ecosystem for prime vulnerabilities; once found, they are exploited to the max for short periods of time. Of note, GhostCat campaigns dominated the spike in phishing attacks that ravaged the Ukraine in February 2022, seeking to cause digital havoc and steal credentials before and during Russia's invasion.

DEFENSIVE MANUEVERS

- **As GhostCat is highly adept at concealing itself, publishers and platforms need the skill of experienced malware analysts who can recognize malicious patterns to thwart major outbreaks, as well as its use as a strategic political and/or military weapon.**
- **GhostCat is a constantly evolving threat, so complete reliance on blocklists to shut down changing attack structures is ineffective. Continuous scanning of inventory via actual mobile devices reveals emerging GhostCat variants among other threats.**
- **With neither creative nor landing page URL within the tag, GhostCat should never pass buying platform audits and should be shut down by exchanges leveraging continuous malware scanning. Platforms and publishers alike should demand tighter security practices from their upstream partners, and should re-evaluate relationships if threats like GhostCat continue to slip in.**

3. Compromised Brand Websites and Landing Pages

While tag-based malware remains a constant presence in the digital advertising space, threat actors are increasingly delivering their malicious payloads through campaign landing pages to circumvent detection. And more and more often, these brand websites are compromised via hacked campaign landing pages of legit advertisers.

Technical support scams like Dolos-3PC lead to backdoor attacks on not only the consumer, but organizations they are associated with, including businesses, government and the military.

The amount of e-skimming attacks has more than tripled since 2020 (Figure 6). Previously, the majority of e-skimming focused on garnering credit card information; however, contemporary attacks collect many types of data—particularly login and other credentials that could be used for more drastic attacks like ransomware, which can also affect their families and corresponding organizations. Protecting consumers is no longer just about making sure an individual is safe.

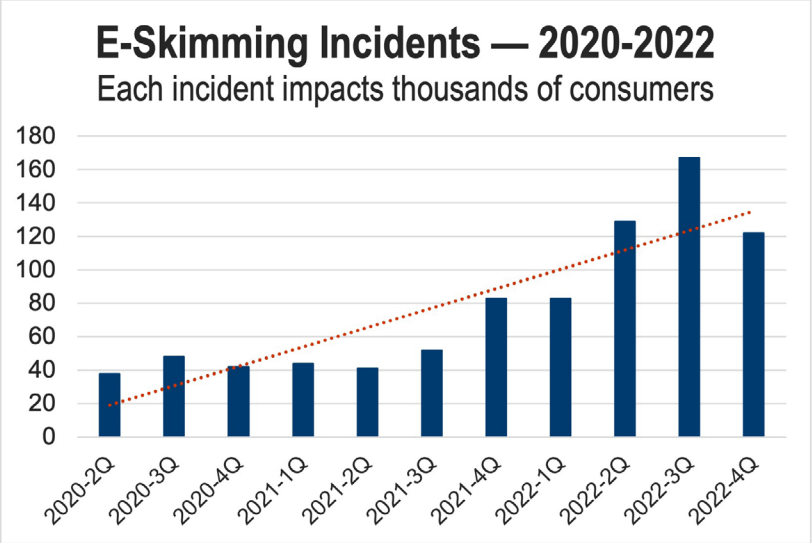

Figure 6: E-skimming attacks rose exponentially in 2022, more than doubling year over year.

E-skimming is not the only attack leveraged on hacked brand websites, apps, and landing pages. The fastest growing named threat in 2022 was MimicManager-3PC, which infiltrates websites through corrupting JavaScript libraries. The presence of MimicManager has grown 3X since September 2022 (Figure 7); the malware is being used by numerous threat actors to distribute a wide variety of backdoors and phishing attacks (including Dolos-3PC).

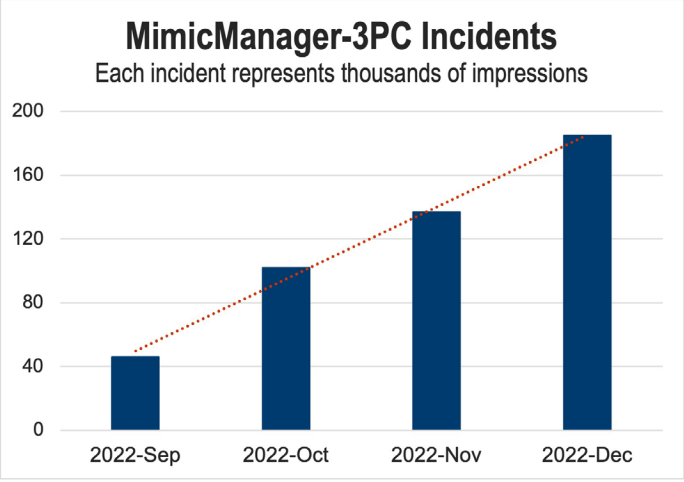

Figure 7: MimicManager was the fastest growing digital threat in 2022.

Some MimicManager incidents are highly targeted, only executing their malicious payload when accessed by specific operating systems or devices. In addition, this malware leverages a sophisticated data collection and processing scheme that allows threat actors to refine their targeting base and better select which malware to serve

consumers—or potentially serve none at all and evade detection (Figure 8).

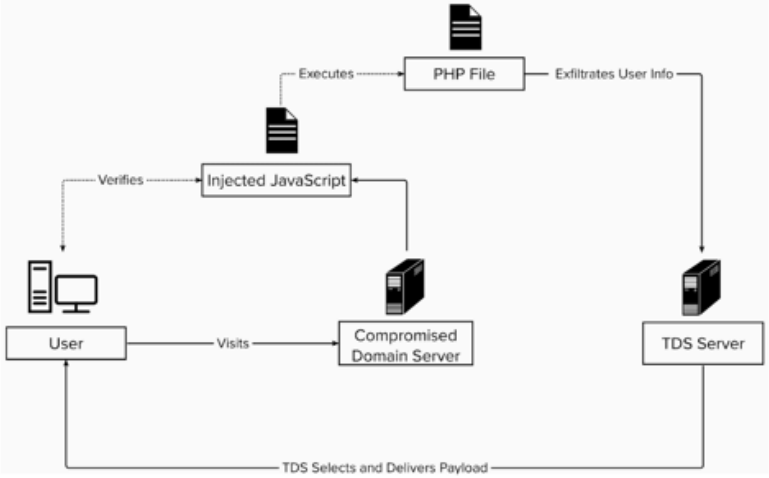

Figure 8: MimicManager's sophisticated data refining process empowers threat actors to improve their data targeting, evade detection by security solutions, and deliver a variety of attacks to consumers.

In an age of economic uncertainty, MimicManager represents a devious cost-cutting ploy for threat actors. Brands buy digital advertising only to have their landing pages serve as malware distribution centers. So the advertisers are also victims—and in keeping consumers safe, publishers and platforms have a duty to rescue them as well.

DEFENSIVE MANUEVERS

- **Due to obfuscation tactics, many advertisers are unaware that their pages/apps have been hijacked. In addition to regular scanning of sites and apps for malware, advertisers must continuously update their content management platforms to defend against breaches.**
- **Because some variants of MimicManager only deliver malicious payloads to targeted devices, clickthrough scanning must employ multiple device profiles (e.g., Android, iOS, Windows) to lure malware out of hiding.**
- **An on-page/in-app creative blocker fueled by top-notch, continuously updated blocklists will stop ads with hacked landing pages from rendering and potentially enticing consumers to click. But ad-supported digital businesses need to inform their upstream platform partners, lest legitimate advertisers continue unintentionally exposing consumers to malware. A centralized platform enabling the sharing of blocking and other malware data can facilitate this.**

4. Exploiting URL Sync Errors

Threat actors are also diversifying attacks by injecting malware into advertising supply chain processes. In late October-early November 2022, a broken cookie sync between two platforms erroneously using the test domain dummy[.]com was exploited to deliver a variety of unwanted content and malware to brand, entertainment, and news/media websites.

Because the unwanted content and malware was delivered via a cookie sync, most on-page/in-app creative blockers were unable to stop the redirects. Thousands of consumers on hundreds of different publishers were affected before the sync error was remediated with the help of The Media Trust.

This barrage was similar to "zombie code" attacks in which threat actors buy or rent domains of defunct businesses (e.g., shuttered platforms) to send backdoors and phishing schemes through syncing URLs. While campaigns exploiting AdTech processes like cookie-syncs tend to be short-lived, they do tend to have impressive reach, assaulting millions of consumers before the vulnerability is identified and fixed.

DEFENSIVE MANUEVERS

- **When submitting campaigns for security and quality scanning, AdTech platforms need to go beyond tags, creative, and landing pages to analyze all code associated with a campaign. This will highlight technical errors that could be exploited by threat actors.**
- **Brands need to periodically review the latent code on their website to identify, analyze and remove unnecessary code as a preventative measure.**
- **On-page/in-app creative blockers have proven ineffective in stopping malware campaigns using syncing exploits. However, publishers are able to detect where the malware is coming from; via their security solution, they can quickly share threat data with their demand partners and shut down these attacks.**

5. Advanced Cloaking and Obfuscation

When it comes to hiding malicious intent, threat actors have become masters of cloaking and obfuscation—and they keep evolving their craft. The cloaking most commonly associated with crypto scheme FizzCore—switching out innocuous creative and landing pages with Bitcoin scams once targeting parameters are met—has expanded to malware campaigns of all stripes. And leveraging thousands of lines of code bloat to bury malicious functions is table stakes.

Specifically, 3 named threats in 2022 scaled new heights in cloaking and obfuscation.

- Chronos-3PC, which compromises brand websites by corrupting JavaScript libraries, actively seeks mobile authentication tokens to ensure that malware is only served to mobile browsers. Beyond that, it also drops the _mauthtoken browser cookie to limit the amount of redirects pushed at a specific consumer—helping lengthen the attack time period by minimizing user disruption. Finally, the attack leverages link shortening and multiple redirects to obscure the ultimate culprit domain.

With malware targeting becoming super granular, scanning with a wide variety of device and user profiles will help unearth even the most heavily concealed campaigns.

- Dolos-3PC's operators created a gigantic portfolio of fake landing pages of various sophistication to give its technical support scam more credibility.
- MimicManager-3PC leverages complex targeting using multiple variables in deciding whether to strike. This not only ensures attacks only hit their marks, but also makes detection difficult.

DEFENSIVE MANUEVERS

- **As threat actors like Dolos feign legitimacy, your security partner must be able to identify attacks through pattern recognition research to halt them before they hit vulnerable consumers.**
- **With malware targeting becoming super granular, scanning with a wide variety of device and user profiles will help unearth even the most heavily concealed campaigns.**

6. E-commerce Scams

As worldwide e-commerce sales continue to grow at an astronomical rate—projected to surpass $6 trillion in 2023—bogus retail operations have flooded ad pipes looking for consumers to defraud. Scam e-commerce company antics range from non-delivery to incorrect delivery of goods with no restitution options.

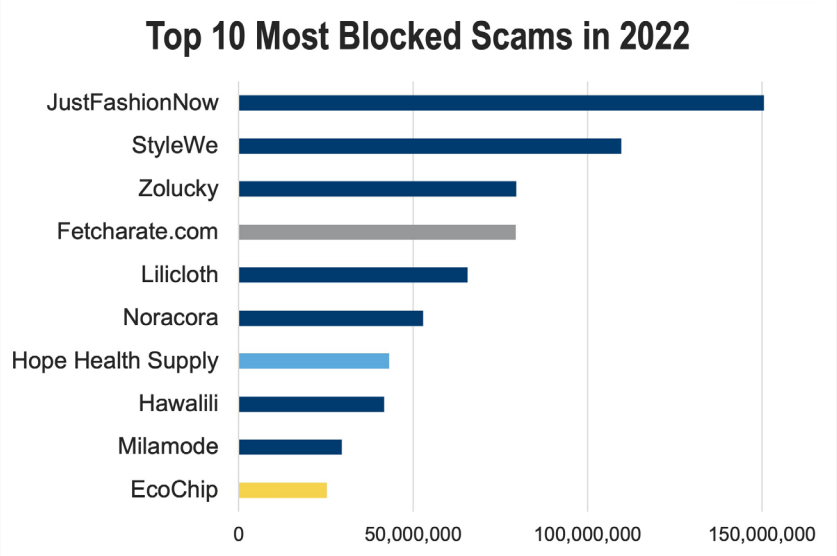

Figure 9: E-commerce scams (dark blue) accounted for 7out of the top 10 most-blocked scams in 2022.

Media Filter, The Media Trust's real-time ad quality solution for publishers, blocked more than 950 million scam ads in 2022, 83% more than the prior year. Around two-third of these blocked scam ads were fraudulent e-commerce sites (Figure 9). The top 3 scam domains blocked in 2022 were not only e-commerce sites, but were also brands run by the same shady Chinese company.

Governments worldwide are tightening regulations around defrauding consumers online. With the forthcoming UK Online Safety Bill and increased investigations by UK Advertising Standards Authority (ASA), British regulators are cracking down on the dissemination of scams to consumers, potentially including platforms, publishers and their AdTech partners. The US Federal Trade Commission is promoting its intention to pursue prosecution of online scam perpetrators. Publishers and platforms should weed out bad actors not just to protect consumers, but also to ensure they avoid regulatory complaints.

DEFENSIVE MANUEVERS

- **The only way to identify e-commerce scams like these online is through thorough security best practices. Make sure your security partner is not only analyzing ads and content for malicious code, but also identifying scam advertisers via research.**
- **On-page/in-app creative blockers are only as good as the blocklists that fuel them. Ensure your blocklist includes scam domains and has the capability to block custom domains that don't meet your brand safety standards.**

7. Sensitive & Regulated Ad Content

After numerous crypto firms made splashy advertising spots for the 2022 Super Bowl, the category presented itself as a legitimate revenue driver for platforms and publishers. Crypto ads quickly became a hot new area of digital advertising; the amount of crypto ads increased by 34% year over year.

But the bankruptcy of FTX and criminal charges filed against its founders and executives seems to have changed industry opinion overnight: crypto advertising blocks by Media Filter more than doubled in the fourth quarter of 2022 (Figure 10).

Publishers souring on crypto ads highlights a growing challenge in managing sensitive and regulated ad content. Many platforms and publishers rely on the IAB Content Taxonomy to govern unwanted/inappropriate ad content; however, the taxonomy lacks a "crypto" category. That schedule was created to classify publisher content, and has been awkwardly applied to ad content with mixed results.

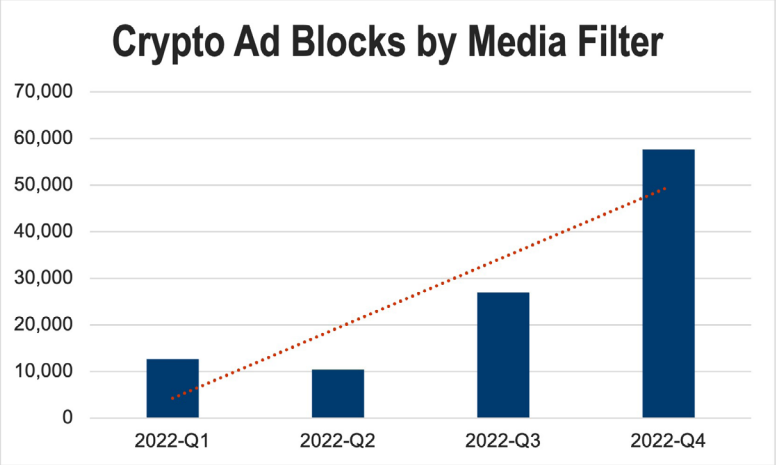

Figure 10: As the scandal around crypto exchange FTX unfolded, crypto ad blocks grew by 114% in 4Q2022.

Still, advertisers, platforms, and publishers are actively using the IAB Content Taxonomy, so a categorization solution needs to be able analyze creatives at scale based on that as well as a proprietary system built to classify ad content. The combination enables platforms to better manage the types of ad content delivered to downstream partners, and empowers publishers to protect their brands and avoid serving unwanted/inappropriate ads to consumers.

OTHER AD CONTENT TRENDS:

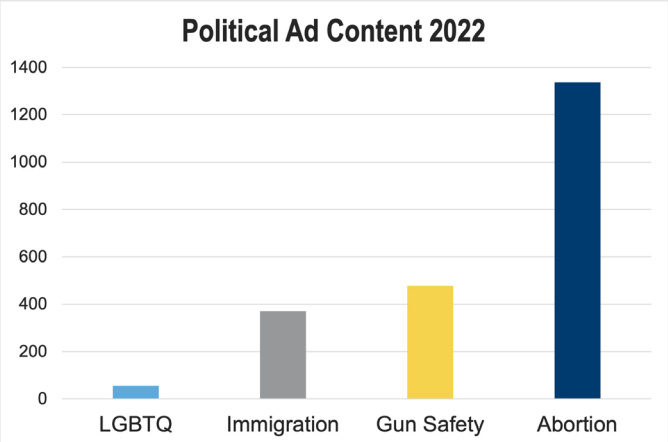

Figure 11: Ads featuring content related to abortion issues were extremely prominent in the digital advertising space before the Kansas abortion referendum in August 2022.

- To add further granularity for platforms and publishers managing sensitive political ad content, The Media Trust added multiple sub-segments to the political category, including Abortion, Immigration, LGBTQ, and 2nd Amendment/Gun Safety. Ads with content referencing abortion (e.g., "pro-life," "pro-choice") were the most frequently detected (Figure 11).

- With numerous US states changing regulations in 2022, gambling ads proliferated throughout digital media, growing 46% year over year. Gambling was the second-most blocked category, following Profane Language (Figure 11).

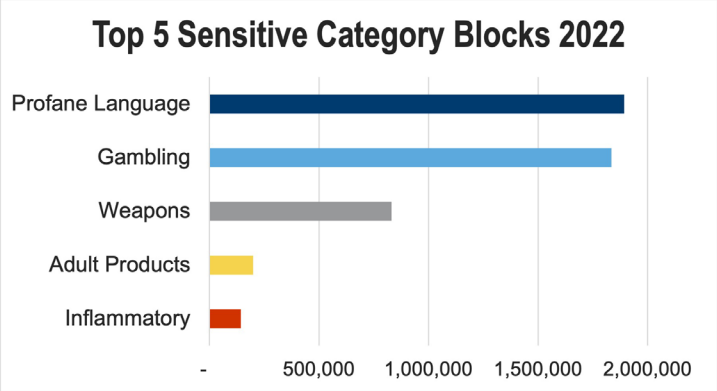

Figure 11: Profane Language, gambling, and adult products were the three categories most blocked by Media Filter in 2022.

- Creative featuring weapons grew 60% year over year, and was the third-most blocked category by publishers.

DEFENSIVE MANUEVERS

When analyzing ads for sensitive and regulated content, AdTech platforms should leverage solutions compatible with the IAB Content Taxonomy as well as classification systems designed specifically to evaluate ad content.

If publishers have concerns about certain sensitive ad content, they should choose to be notified when that category appears on their sites/apps. Furthermore, their ad quality partner should furnish a creative gallery enabling publishers to block specific ads that are brand unsafe or potentially offensive to consumers.

During the 2022 US election season, The Media Trust Ad Categorization solution cataloged twice as many political ads as in 2021, but only slightly more than the 2020 election.

Threats on the Horizon

Threat actors are constantly evolving, and their advances in 2022 were truly disquieting: improved targeting of vulnerable Internet users like the elderly and children as well as diversified attacks through URL syncs and hacked brand websites and landing pages. Here are four other areas to keep a watchful eye on as 2023 progresses.

Cryptojacking: Even if the value of many cryptocurrencies took a serious dive at the end of 2022, deploying cryptomining malware is a lucrative and fast-growing enterprise. The potential attack surface continues to expand, with more and more devices connecting to the Internet each day.

Increased Mobile Targeting: Apple's App Tracking Transparency has decreased the amount of third-party targeting data in iOS apps, which in turn has reduced CPMs. This is one of many opportunities for threat actors to attack consumers on their personal devices. Publishers and app developers need to ensure they have protective measures in place as they are the last line of defense for vulnerable consumers.

Governments and Political Actors Leveraging Malvertising Tactics: Platforms and publishers are increasingly pushing back on state actors and political groups that seek to use advertising to spread disinformation. Considering that state actors already use malware as a weapon (e.g., the Ukraine conflict), the next step in distributing disinformation is using cloaking and obfuscation tactics to evade detection and target impressionable consumers.

Threat Actors Scaling With AI: AI image creation and chatbots provide great diversion, but they also can be used by threat actors to easily build creatives and landing pages at scale, making it hard to shut down complex malware assaults. Fortunately, AI is also an extremely powerful tool for detecting patterns in malware deployment.

Recommendations for Covering Your Assets

STAY VIGILANT

With economic uncertainty comes the call to cut costs—but sacrificing digital security for cost savings can have dire consequences. Threat actors are anticipating digital companies will let down their guards and are already probing for vulnerabilities. Monitoring websites and apps for security breaches in addition to advertising is crucial for protecting consumers. Never forget that the safety of digital consumers is key to the success of your business.

INCREASE SCRUTINY

Threat actors are constantly improving their obfuscation tactics, including hiding their malicious intent via cloaking and using innocuous creative/imagery and code to fool security audits. They're increasingly using hacked landing pages of legit advertisers to spread a variety of malware. Weeding out threats—and rescuing victimized advertisers—requires continuous review from a variety of device profiles and analysis of tags, creatives, clickthroughs, and landing pages. Publishers need to pay additional attention to reporting from their on-page/in-app blocker to determine which demand sources are spreading malware.

GET CONNECTED

The ingenuity of threat actors is highlighting the limits of on-page/in-app blocking of malware and unwanted ads. Digital publishers, AdTech platforms, e-commerce companies and even enterprise brands with consumer-facing websites need fluid communication channels to share and quickly remediate incidents as they flare up to maintain revenue. Keeping consumers safe requires digital companies to get closer, better know each other, and work more effectively with each other.

About The Media Trust

Today's digital ecosystem relies on The Media Trust to safeguard the consumer experience. We fix the issues that harm your customers, drive data breaches, violate regulations, impede revenue, and tarnish your brand.

Acting as your audience, our unique digital safety platform captures their true user experience and stops harmful activity so you can better monetize and govern your digital assets.

Since 2005, hundreds of digital businesses have depended on The Media Trust to protect their strategic digital revenue channels. Why not yours?

The Media Trust—your partner in digital trust and safety.

Learn more at www.mediatrust.com.

For a demo, reach out to: info@themediatrust.com

January 2023

THE MEDIA TRUST
Digital Safety. Delivered.