CYA* 2022

7 Deadly Malware Trends

Analyzing alarming growth in ad industry malware to offer defensive strategies for securing revenue and protecting consumers

*Cover Your (Digital) Assets

THE MEDIA TRUST

We know digital security.

The Malware Explosion Continues

As premium advertisers shift spend to channels like connected TV and private marketplaces, bad actors are flooding open programmatic display marketplaces to assault AdTech platforms, publishers, and consumers with a wide variety of malicious content. The amount of malware in the digital advertising ecosystem surged to colossal levels in 2021, making it harder than ever for platforms and publishers to both drive revenue and ensure consumers' digital trust and safety.

Since 2016, malware in digital media has grown almost fivefold (Figure 1), with the steepest increases occurring in the last two years. At the beginning of the pandemic in 2020, malvertisers hit the digital advertising markets hard as advertisers pulled back spend. This growth

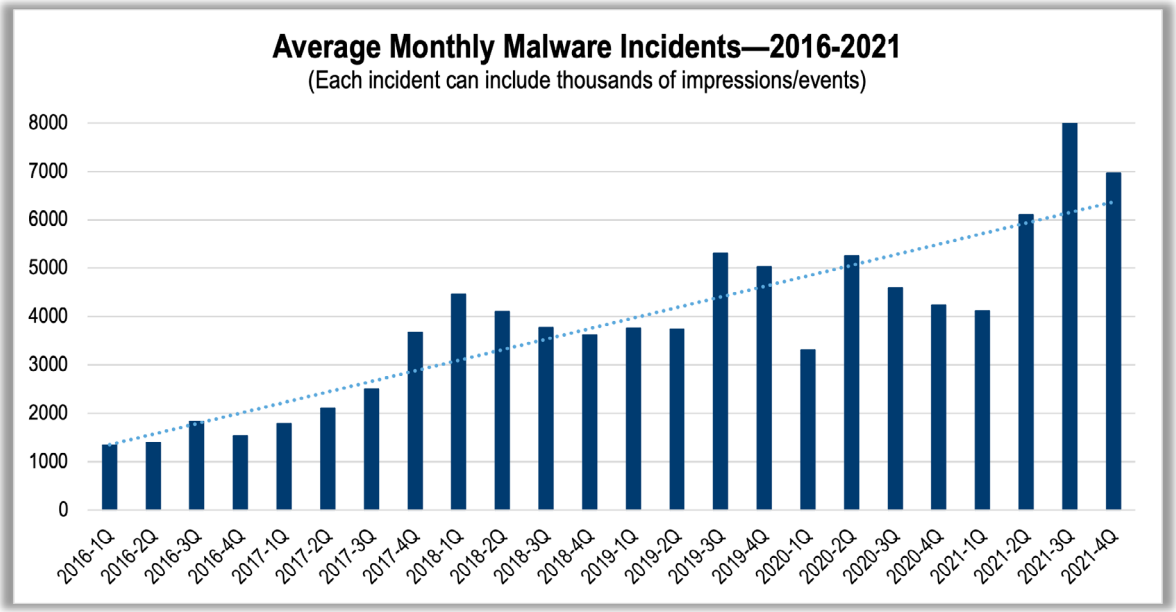

Figure 1: The amount of malware in digital media has grown steeply since 2020.

paled in comparison to the 2021 explosion in malware (Figure 2) detected by The Media Trust's Digital Security and Operations team, signaling an increased weaponization of the digital advertising ecosystem to harm consumers around the world. Third quarter 2021 in particular saw an incredible rise in malware, almost doubling year over year.

This is alarming in the wake of numerous high-profile ransomware attacks in 2021—including Colonial Pipeline, JBS Foods, and Kaseya—that had extensive effects on consumers and businesses. Major corporations and governments are under siege from tenacious threat actors, with hybrid in-office and remote workforces especially vulnerable. Malvertising is not only an attack vector for ransomware, backdoors, keyloggers, and other grievous threats—it can also provide data and device access for future large-scale assaults.

Key Stats for 2021

Throughout the year, Digital Security and Operations identified:

- **26,664 new malware incidents in 2021, a ~30% increase over the number cataloged in 2020. Each incident accounts for thousands of malicious impressions or events.**
- **~2,200 malware incidents managed daily, on average; 64% increase over 2020.**
- **3,000+ daily malware incidents managed during the summer—the height of the 2021 malware blitz.**
- **4X increase in blocked malvertising incidents via Media Filter, The Media Trust's real-time ad-quality solution, compared to 2020.**

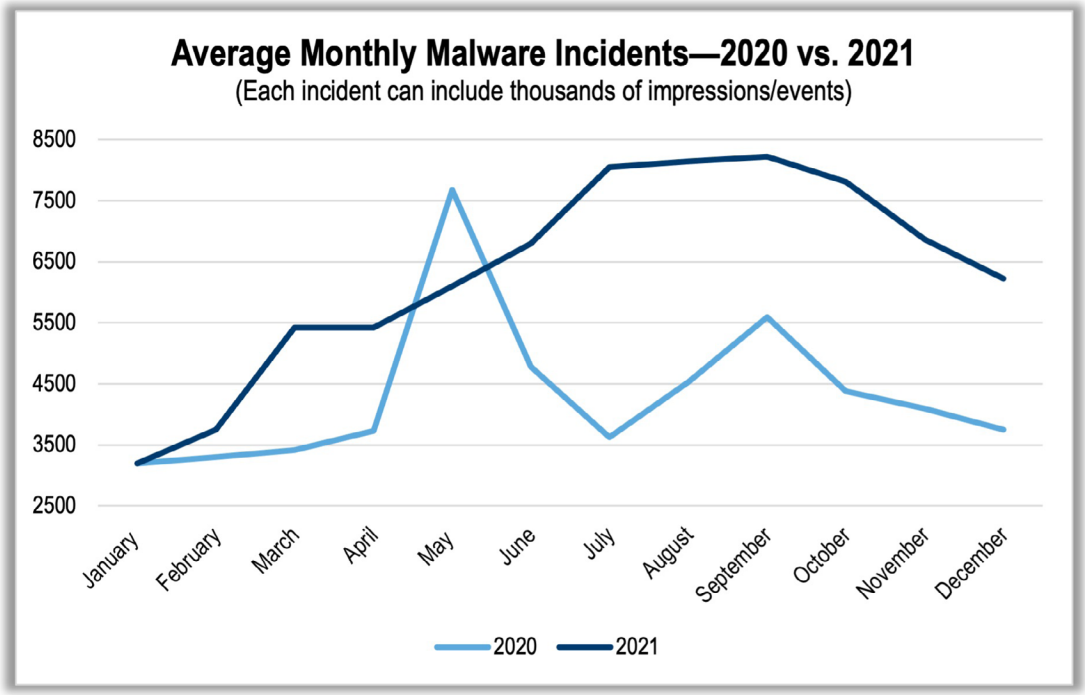

Figure 2: While malware in the digital ecosystem spiked at the outset of the pandemic, the steady growth throughout 2021 was even more dramatic.

No one style of malware stood out during 2021. The year was a smorgasbord of digital malevolency across a range of attack vectors, including:

- **1.7X growth in redirects between January and October**
- **Expansion of clickbait-based malware, including a 23% increase in FizzCore**
- **63% surge in scam ads, which made up a third of malware detected**
- **2.2X hike in compromised landing pages through July, with many legit small and medium advertisers unaware of hacked sites**

Publishers and platforms alike rely on the open programmatic marketplace for their livelihoods, but protecting consumers in this increasingly treacherous environment means employing a super-assertive ad quality strategy powered by a comprehensive set of tools. Also key is keeping abreast of malvertisers' latest tactics—as well as sharing findings and insights with peers to promote a safer ecosystem for consumers.

Are Creative Blockers Failing Us?

Since they rose to prominence among publishers in 2017, creative blockers have been widely heralded as the ultimate solution for beating back the malware menace and for protecting consumers. However, the amount of malware in the digital media space has increased 3X since 2017—instead of stamping out malware in digital advertising, the problem has (exploded) and consumers are more at risk online than ever before. Which begs the question—do creative blockers work?

The answer is more complicated than industry practitioners likely want to hear. Yes, creative blockers work, but they're only as good as the malware data being pumped into their blocklists.

Recent analysis found that Google Safe Browsing detected only 2% of the malicious domains found by The Media Trust's Digital Safety and Operations Team.

Too many blockers only stop ads being served by so-called "high-risk platforms." There is no industry standard around what makes a platform "high-risk," and malvertising is just as prone to come through "premium" platforms thanks to malvertiser ingenuity around cloaking and evasion. For a creative blocker to be effective and precise, blocklists must be based on exhaustive forensic analysis of creatives, tags, and landing pages at scale. Skilled analysts can pick up on code, creative, and domain patterns to unearth well-concealed malvertising.

To ensure data fueling creative blockers is as fresh as possible, first-party data from in-house malware analysts will always be superior to third-party data. For example, a recent analysis found that Google

Safe Browsing, which aims to protect consumers from visiting unsafe properties, detected only 2% of the malicious domains found by The Media Trust's Digital Security and Operations team.

Over-reliance on creative blockers—especially ones focused on "high-risk platforms"—at the expense of scrutinizing creatives, tags, and landing pages is a recipe for disaster. And arguably that is what's happening right now with the steep increase in malware in digital media.

Security solutions need a healthy balance of blocking and ad scanning to enable safe environments for consumers, and beat back bad actors flooding the ad pipes with malware.

Safeguarding 2022: 7 Malvertising Trends

This report will help you "Cover Your Assets" (the digital ones!) in 2022 by detailing the seven most prominent malware trends. We'll also share proactive measures for mitigating each threat, aiding you in keeping digital consumers free from harm.

1. Ubiquitous Cloaking

Think you know malware when you see it? Well, that depends on whether you actually see it. The vast majority of malicious campaigns now employ cloaking tactics: fingerprinting to detect and evade testing environments, and then identify target environments for maximum impact. Be aware: a high percentage of malicious code is actively checking for the presence of malware detection tools and creative blockers.

Through cloaking, a piece of malvertising will employ portfolios of innocuous creatives and landing pages to evade platform creative audits. Once in the advertising pipes, malicious payloads are only served when fingerprinting ensures an ad is in the desired environment—e.g., an app on an Android. This makes them increasingly difficult to identify and more likely to proliferate.

The most notorious abuser of cloaking is named threat FizzCore, which assaulted consumers en masse all year but was near omnipresent in the digital ecosystem throughout July (Figure 3).

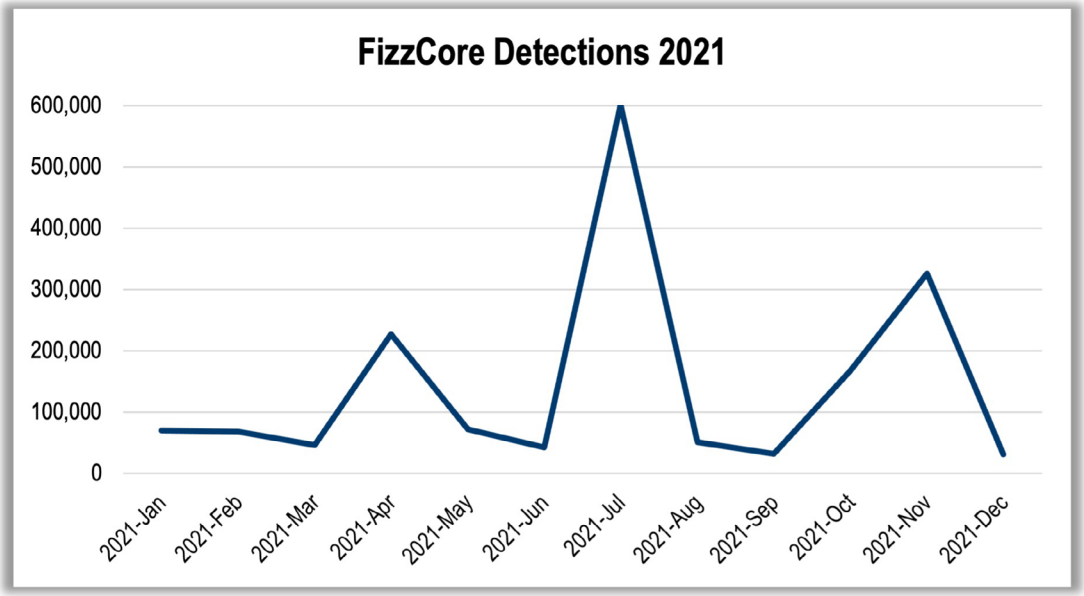

Figure 3: The digital advertising ecosystem was awash in FizzCore malicious clickbait in 2021, with major outbreaks in April, July, and November.

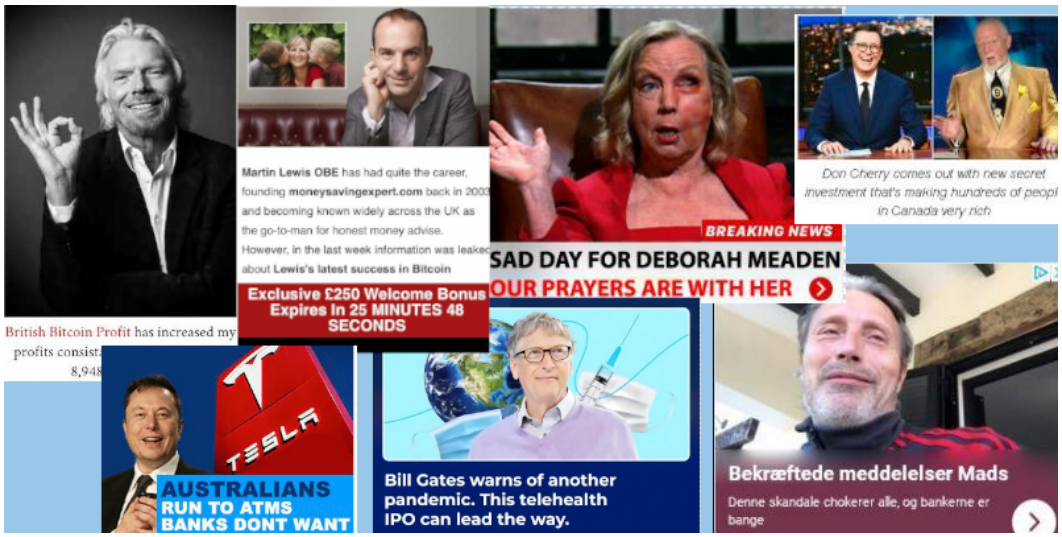

Figure 4: Richard Branson, Martin Lewis, Elon Musk, and Elon Musk are just a handful of the celebrities hawking sketchy schemes in FizzCore ads.

Malicious FizzCore creative is most infamous for featuring celebrities like Richard Branson and Elon Musk endorsing bogus Bitcoin investments, but the malvertising (and its growing legions of copycats) has branched out into hawking renewable energy investment schemes among others (Figure 4). FizzCore has been a chief driver of UK efforts to enhance regulations against online scam advertising, potentially expanding liability to publishers and platforms.

DEFENSIVE MANUEVERS

- **Publishers and platforms must scrutinize all ad components—creative, tags and landing pages—passing through their environments.**
- **Malicious code has a harder time hiding true intent with client-side creative scanning—analysis via a network of actual devices with a variety of browser, geography, and user profiles.**
- **FizzCore and similar malware copy or re-use innocuous creative. Malware teams using AI image analysis identify these at scale and upload new malicious campaigns into a creative blocker.**

2. Rapid Domain Cycling

Malicious redirects grew 1.7X between January and October (Figure 5), and key to this resurgence was rapid domain cycling. As soon as one domain serving malicious code was detected and neutralized, the malvertising switched to another to deliver payloads.

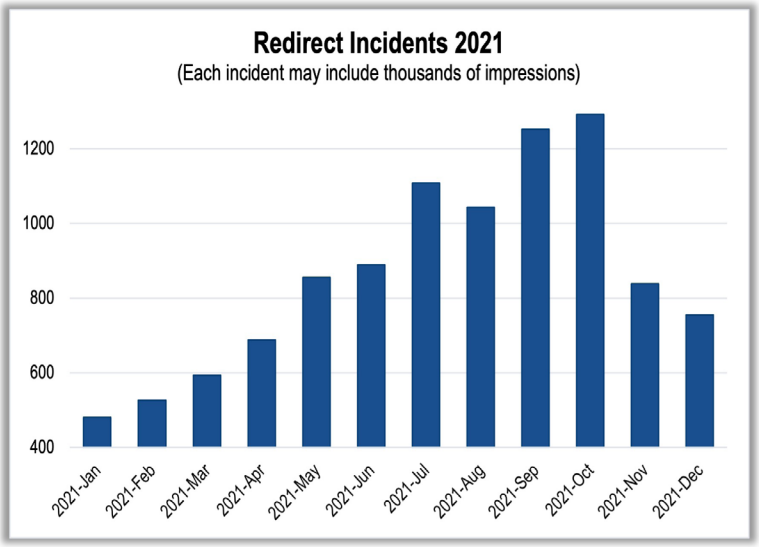

Figure 5: Digital advertising redirects steadily ascended throughout 2021 before peaking in October.

The result is seemingly unkillable malvertising campaigns, with malware analysts continuously keeping abreast of emerging domains in order to keep consumers safe and revenue flowing.

During a barrage in May that affected more than 1,000 publishers across the U.S. and Europe, The Media Trust's DSO detected more than 30 active domains and another 25 dormant ones from the same lineage cycling in and out of campaigns across multiple platforms. Malvertisers are increasingly using multiple primary domains, and inflating their supply with 10 or more top-level domains (e.g, .world, .xyz, .online).

DEFENSIVE MANUEVERS

Bad actors heavily rely on free web-hosting platforms such as GitHub to host scores of domains. Highly experienced malware analysts can identify suspicious domain trends and even predict dormant domains that will be used to prolong the malware attack.

3. Scampocalypse Now

Scams accounted for nearly a third of all malware detected by The Media Trust and grew 63% throughout the year. While most malvertising trends downward at the end of the year because Q4 programmatic pricing is too rich for bad actors' blood, scams actually jumped 9% during the quarter thanks to a barrage of "gift guide" ads pushed by sketchy retailers (Figure 6).

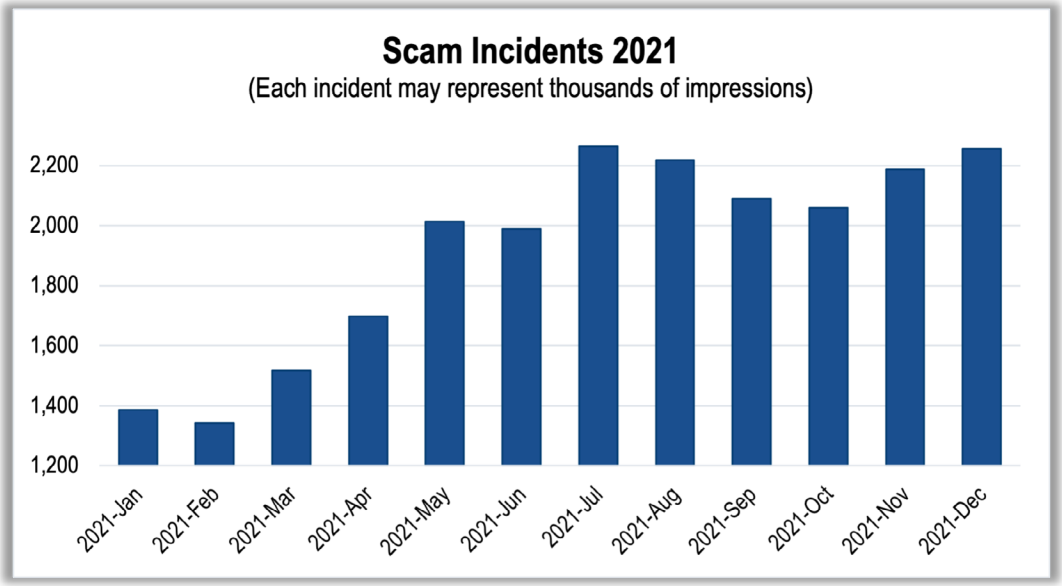

Figure 6: Scam incidents peaked in July, but managed to stay high even in the fourth quarter, when malware typically subsides.

There is no industry agreement on what connotates a "scam." The Media Trust defines a scam as a campaign that employs deceptive information to encourage users to enter personal information for retargeting and reselling purposes, and/or using false claims to sell products—basically, activity that harms consumers.

The content of scams ran the gamut in 2021 (Figure 7): data-leeching lead generation operations in the mortgage and home solar industries; sketchy green energy investment schemes; vitamin supplements greatly exaggerating health benefits; clothing outlets that fail to deliver purchases; and more.

Scam ads should be on all malware radars because it's a short leap to something far more malicious. The aforementioned FizzCore started as a more straightforward bitcoin scam before employing cloaking technology to fool DSP creative audits and expand its reach—astronomically.

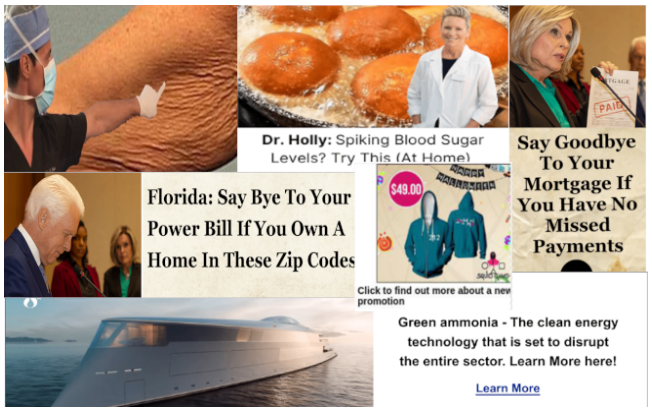

Figure 7: Scam incidents peaked in July, but managed to stay high even in the fourth quarter, when malware typically subsides.

With most malware, the proof is in the code; however, identifying scams requires additional diligence. Ideally, platforms would research their buyers/advertisers to weed out scammers, but the need for scale often supercedes this duty. In reality, publishers are forced to communicate ad quality priorities and it's up to the platforms to comply or face consequences.

Unfortunately, many platforms and publishers are willing to look the other way as scam ads pass through the pipes and pocket the revenue, the modus operandi seems to be: "Clicker Beware." That's an unhealthy attitude that leaves consumers vulnerable and digital media unsafe. As ad quality grows in prominence for revenue efforts—and regulators become increasingly bold in protecting consumers—publishers and platforms will have little choice but to excise scams.

DEFENSIVE MANUEVERS

- **Platforms: perform additional diligence on advertisers and buyers to ensure businesses are above-board.**
- **Publishers: Develop an acceptable creative policy and ensure ad quality provider identifies scams and adds them to blocklists.**

4. Testing, Testing— Is This Thing On?

To the misfortune of the digital media landscape, malvertisers have greatly increased their sophistication over the last several years. The continued surge in malware incidents in 2021 can be partially attributed to many short-lived campaigns seeking vulnerabilities in the advertising pipes. Once weak points are discovered, either bad actors rush to bombard or activate sleeper campaigns.

For example, between January and April 2021, incidents of mobile-focused phishing malware GhostCat-3PC increased 65% before declining in May. But right on cue, the digital advertising space was bombarded with GhostCat campaigns in May; the testing period complete, the barrage began (Figure 8).

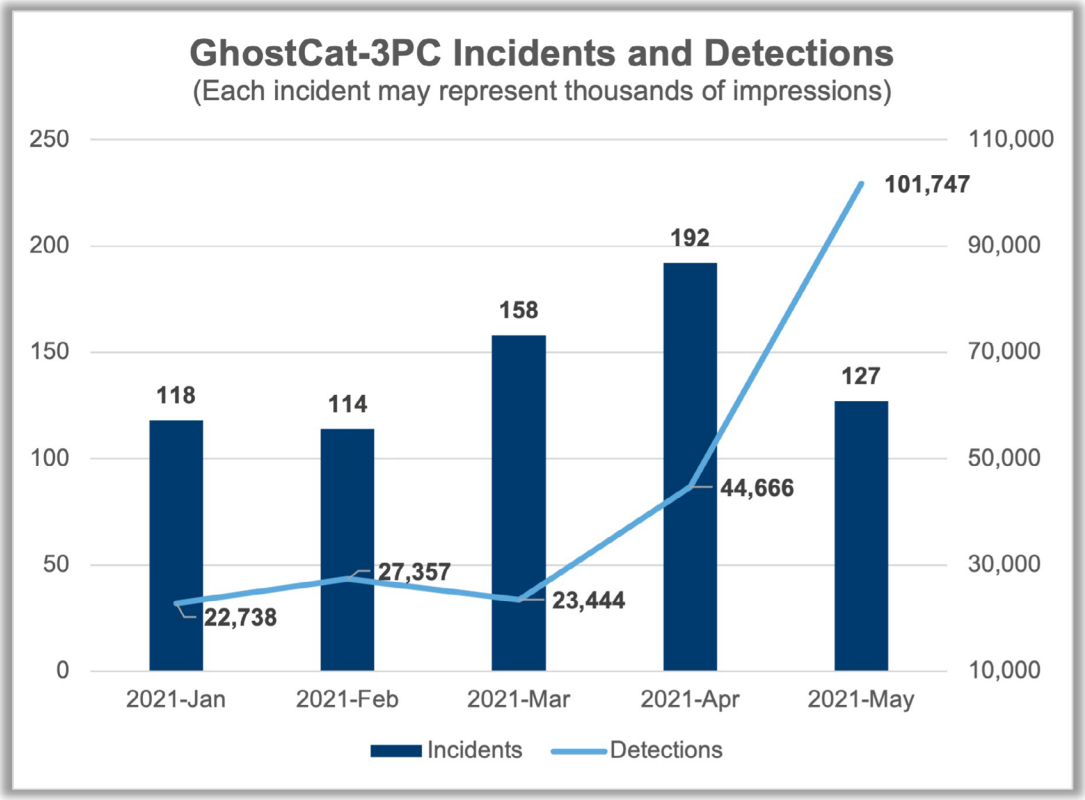

Figure 8: Right as the number of specific incidents peaked in April, a surge of malicious Ghostcat-3PC campaigns hit the digital media landscape in May.

To further evade detection and elude malware hunters, bad actors will deploy campaigns with innocuous creatives and landing pages for long time periods before suddenly turning them on. Sometimes these will be aimed at certain devices or browsers, other times just active for specific geographies. Numerous short tests are also meant to throw malware hunters off the scent of longer-running campaigns that have yet to be detected.

DEFENSIVE MANUEVERS

- **Re-analyzing inventory is key for spotting a variety of anomalies (e.g., technical issues, newly compromised landing pages), but can be a lifesaver if it turns up a sleeper malware campaign before it wreaks havoc on the industry.**
- **Because malvertisers often steal or reuse creative, previously observed images as well as domain patterns can alert analysts to suspicious activity. A crack malware desk can identify suspect campaigns in the wild using AI to aid detection.**

5. Compromised Landing Pages

Just as malware doesn't stop at the creative, malware analysis can't call it quits at the tag.

Often, danger to consumers is only a click away. The Media Trust detected gigantic spikes in compromised landing pages during summer 2021 (Figure 9) featuring different attack types, e.g., redirects, phishing, parked domains, exploit kits, etc. June witnessed a massive jump in phishing landing pages (6.3X the month before) while the amount of fake software install pages rose 6X between May and July.

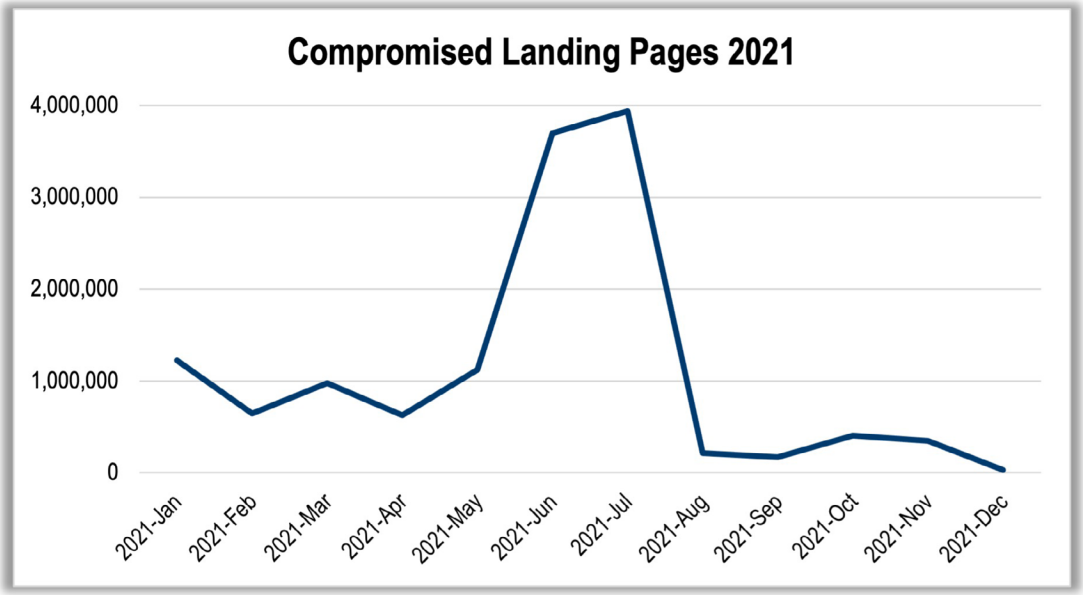

Figure 9: Small and mid-sized advertisers were greatly impacted by a surge in compromised landing pages in summer 2021.

Many of these compromised landing pages were hijacked from legit advertisers. Small and medium-sized businesses that outsource their web design are especially vulnerable to bad actors if their web publishing software falls out-of-date. Often advertisers are completely unaware that landing pages are compromised until their ad partners come to the rescue.

Just as malware doesn't stop at the creative, malware analysis can't call it quits at the tag. Furthermore, finding hacked landing pages for important advertisers is a great service and will help you secure future business.

DEFENSIVE MANUEVERS

- **Platforms and publishers must examine go beyond tag and creative analysis to evaluate click-throughs and landing pages**
- **Client-side scanning from a variety of geos and device profiles can thwart cloaking attempts to disguise malicious pages.**

6. Creative & Landing Page Not Included

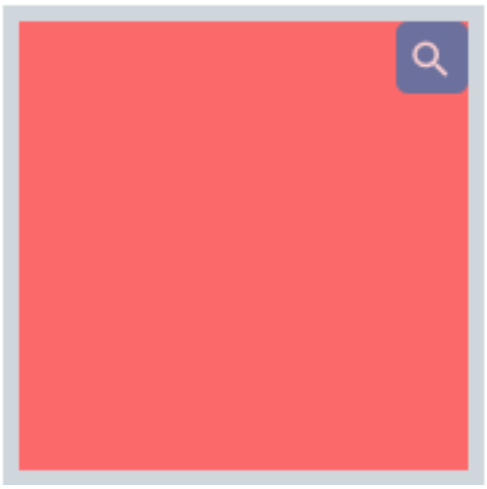

Figure 10: When appearing in a non-target environment, Ghostcat serves this pink box.

GhostCat employs thousands of lines of inoperative code in an attempt to obscure its malicious intent—phishing schemes or even harmful software downloads.

However, recent variations take this a step further and discard both creative images and landing pages within the tag, GhostCat only serves its malicious payload in a target environment confirmed by fingerprinting; if the malware misses this target, a mysterious pink box appears in the ad unit (Figure 10).

This "obfuscation by omission" makes it harder to stop campaigns before they wreak havoc on platforms and publishers. Malware analysts typically study creative and landing page patterns to identify emerging assaults, so running campaigns without creative or landing pages helps GhostCat evade detection and breach more consumer devices.

Ad platforms like SSPs should examine what upstream partners are delivering this kind of malware. An ad campaign without creative or a landing page should never be able to pass a DSP's initial audit. If an upstream partner is not performing the barest amount of diligence, the working relationship needs to be re-evaluated.

DEFENSIVE MANUEVERS

Continuous scanning of tags reveals malware lacking creative images or landing pages.

7. Zombie Code

It may seem hard to believe, but not all malvertising is delivered via ad server. A growing source of redirects and other malware is user-sync URLs from domains associated with defunct AdTech companies.

Bad actors are buying or renting dormant domains from out-of-business AdTech firms such as Revenue Science, Choicestream, and Telemetry, and then sending malware directly through the user sync (Figure 11). Publishers and platforms falling victim to these schemes have outdated code and are still calling to deceased partners... that frighteningly spring back to life.

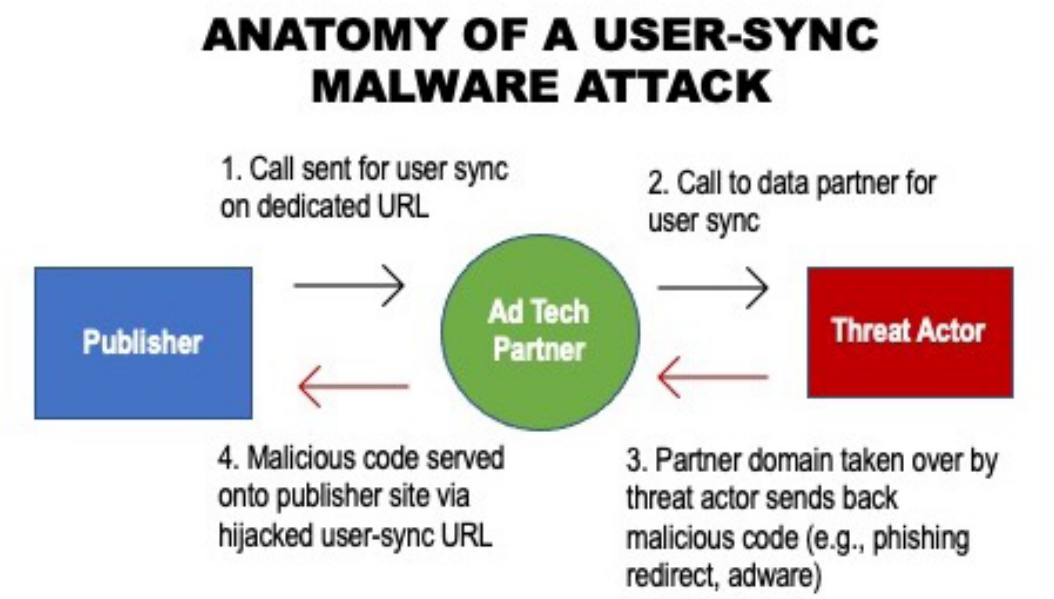

Figure 11: The February Electrum attack used a corrupted user-sync URL to serve redirects rather than an ad server.

So-called "Living Dead AdTech" or "zombie code" can lead to brief yet brutal outbreaks: in February 2021, Electrum-3PC bypassed creative blockers to deliver more than 24,000 redirects via user-sync URLs. Peaking in five hours, the attack circled around the globe and affected 450+ publishers and platforms.

While the majority of outbreaks detected by Digital Security and Operations have delivered redirects, the potential to deliver ransomware or other more severe malware is unnerving—especially as many creative blockers seem helpless to stop these attacks.

DEFENSIVE MANUEVERS

- **Platforms and publishers need to periodically dive into their code and remove domains of partners they no longer work with—especially if a company has ceased to exist.**
- **Publishers should scrutinize all outgoing and incoming calls to and from their properties to check for unauthorized vendors. This includes archived pages, which often fall prey to zombie code.**

Conclusion

As the amount of malware in the digital media space continues its meteoric rise, AdTech platforms and publishers need a multifaceted defense to keep consumers safe.

With advertiser spend increasing at a higher rate in channels like connected TV and private marketplaces, the open programmatic marketplace is ceding more and more territory to malvertisers. Fortunately, ensuring consumers' digital trust and safety aligns well with protecting and even growing revenue as ad quality becomes an increasingly important factor in a hyper-competitive digital media landscape.

The quality of analysis behind your tag and landing-page scanning and your creative blocker can often be the difference between a costly malware outbreak and benign ad experiences for consumers.

Mitigating the impact of bad actors means leveraging a full suite of tools for security and ad quality, including:

- **Ad tag analysis by a variety of geographies**
- **Clickthrough and landing page scrutiny**
- **Continuous site monitoring to discover emerging and evolving anomalies and non-ad-based malware**
- **Creative-blocking through blocklists fueled by original-source malware data updated in real time.**

But tools are not enough—behind the scenes, a dedicated crew of experienced malware analysts should be employing cutting-edge detection tools and hunting down malware in the wild. The quality of analysis behind your tag and landing-page scanning and your creative blocker can often be the difference between a costly malware outbreak and benign ad experiences for consumers.

Balancing revenue efforts and consumer safety will only become more difficult as malvertising proliferates. But platforms and publishers that recognize their responsibility to consumers and the overarching threat of malware are prepared to face the challenge and thrive.

About The Media Trust

The Media Trust is fixing the internet by creating better digital ecosystems to govern assets, connect partners and enable digital risk management. Established in 2005, The Media Trust operates as a digital safety platform by leveraging a physical presence in more than 100 countries and 550 locations to detect and remediate security, privacy, ad quality and performance violations executing on websites and mobile apps that harm consumers. More than 600 media publishers, AdTech platforms, agencies, retailers and enterprises—including 40 of comScore's AdFocus Top 50 websites—rely on The Media Trust to protect their digital environment, revenue, brand reputation, and, most importantly, consumers. Learn more at www.mediatrust.com.

To evaluate properties and ads, reach out to: info@themediatrust.com

January 2022

THE MEDIA TRUST

We know digital security.