THIRD-PARTY CODE: The Number One Driver of Malvertising

3PC

Internet users have always been targeted by malware which compromises their personal and financial information, but the biggest threat sources have changed with time. As Cisco highlighted in a report published earlier this year through the Talos Intelligence Group, today's web is vulnerable to payloads that spread through malicious advertising (malvertising). Symantec also notes in its 2019 Internet Security Threat Report (ISTR) that 26.4% of organizations have been impacted by malvertising via mobile applications.

Although malvertising has been on the rise for at least half a decade, both reports leave out one crucial detail: how unseen and unregulated third-party code (3PC) aids malvertising's spread across the Internet. Until organizations are equipped to control the third parties executing across their websites and mobile apps, remedies for malvertising will remain superficial at best while 3PC continues to threaten the digital ecosystem's long-term viability, leaving Internet users exposed to data theft, phishing attacks and more.

1. MALVERTISING IS A GROWING DANGER

Online advertising is big business: this year, Ad Tech will rake in $725 billion across the globe. Unfortunately, that fuels the malvertising business too. In today's always-connected world, reaching victims through an innocuous banner advertisement is all too easy, and incentives range from profit to political manipulation to espionage.

The payload of a malicious ad varies from campaign to campaign, but common attacks include:

- **BAD REDIRECTS:** users are forced to visit a compromised website
- **FAKE NEWS:** users are exposed to misinformation with the goal of manipulating their views, i.e., political, social, economic and more
- **PHISHING SCAMS:** users are directed to fake homepages of familiar brands to steal financial or login information
- **CRYPTOJACKING:** user devices are hijacked by malware to mine cryptocurrencies

This year, the number of malicious ads has grown by 150%: in the past few months, a single malvertising campaign originating from Hong Kong exposed Internet users to 100 million compromised ads serving up redirects – and that's just one incident. Using our platform The Media Trust team detects and manages more than 1,000 active threat incidents per 24 hours, and classifies more than 5,000 new malicious domains each month.

2. KILLING ADS IS NOT THE ANSWER

When the problem of malvertising comes up, it's tempting to blame online advertising itself. But the digital economy needs Ad Tech, as Cisco's report recognizes:

"ADVERTISING IS A KEY PART OF THE INTERNET AS A WHOLE....IT ALLOWS PEOPLE TO SUPPORT THEIR PASSION PROJECTS, THEIR SMALL BUSINESSES, AND THE FOOD BLOGS OF PEOPLE AROUND THE WORLD".

Today, the very publishers who are threatened by the existence of malicious ads also depend on ads for revenue. Without them, the Internet wouldn't be free, and user growth would rapidly decline. We've already seen how the AdBlock crisis forced news organizations to adopt the less lucrative paywall model: that's what happens when all legitimate ads are conflated with bad ads.

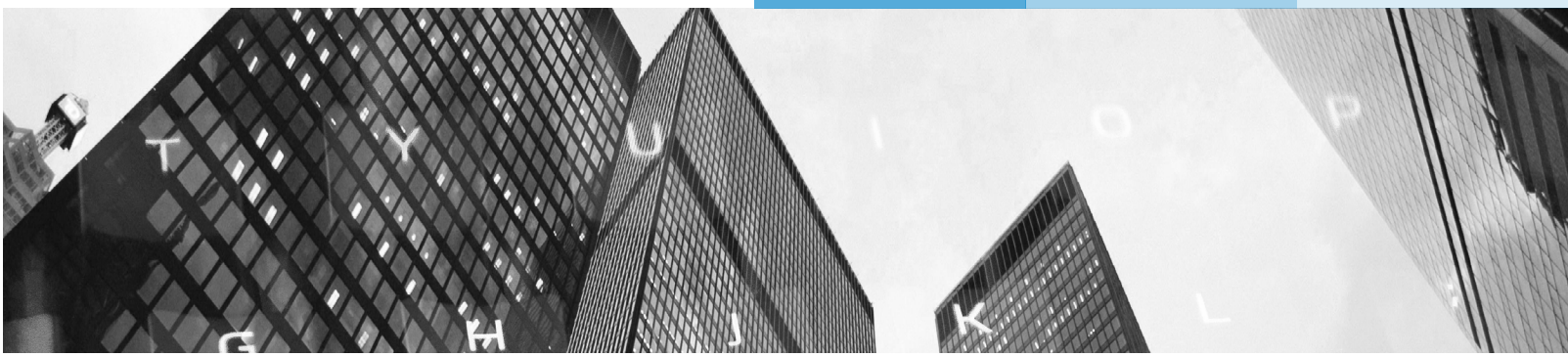
Now, many publishers who are aware of malvertising have been drawn into a similar scheme through the rise of enterprise blockers that promise to prevent bad ads from executing. Not only is this solution rarely effective (blockers are consistently behind malware spread), but it tends to kill many legitimate ads in the process, strangling publisher revenue and hurting UX.

3. MALVERTISERS HAVE THE UPPER HAND

In one case study referenced by Cisco, a malicious ad was found to contain advanced code allowing it to bypass client-side blockers. This is nothing new: as Verizon points out in its 2019 Data Breach Investigations Report (DBIR), attackers change up their tactics in response to new technologies. Likewise, malvertisers have been able to reverse engineer and dodge blockers for some time. Not only do they have multiple paths into the digital supply chain, but many different methods – client and server side – to execute on user devices once they're in.

Using polymorphic code and geographic targeting, malvertisers can also adapt an ad to any situation or user profile. On one domain, it blends in and behaves normally; on another domain, it drops a payload specifically designed for the device it's running on. When malicious buyers are identified and banned from DSPs, they quickly move on to a new provider, and continue their work.

With this much agility and skill, it's no surprise that we find malicious ads running on Alexa 500 domains every day. The game has changed in favor of malvertisers, in part because organizations have tried to treat a symptom rather than the underlying cause. Fortunately, there is a cure – and it begins with controlling 3PC.



3PC AND THE DIGITAL SUPPLY CHAIN

The crucial detail missing from everyone's radar is this: today, organizations don't control the code running on their digital properties. In fact, 80-95% of media and e-commerce source code is owned and operated by an entity other than the host organization. This lack of control and operational insight provides the ultimate backdoor for malware to execute and spread.

A quick look at one publisher site revealed third-party partners which comprised more than 88% of executing code. In addition, we noted:

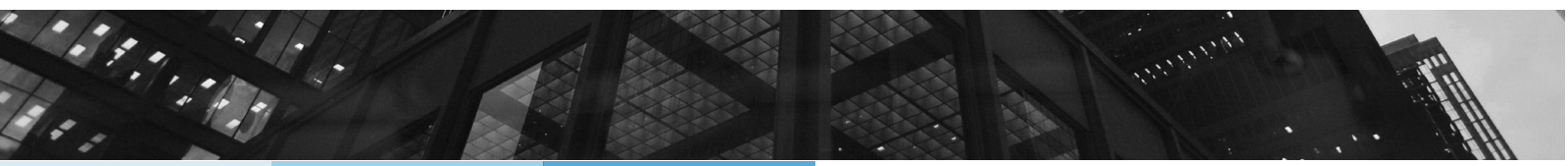
- **Calls to 212 domains, of which only 39% were approved or identifiable by the organization**
- **5% of the domains classified as suspicious, and malware incidents were detected on at least one page**
- **Phishing attempts were launched in the form of fake surveys on another page**
- **9 domains originated from a foreign country**

While 3PC—like advertising—plays an important role in the digital economy, not all of it is benign. And unlike advertising, 3PC goes largely unregulated. Where most organizations are concerned, these assets constitute shadow IT that runs in the background far from scrutiny even though they are directly connected to users and sensitive data resources.

TAKING BACK CONTROL

The connection between malware and third-party code is not theoretical. When organizations take inventory of their digital assets and conduct regular scans to remove and report bad partners upstream, malware events go down: in one case, our client experienced a 36% reduction within a week of hiring a new CISO.

Maintaining control of technology resources, vetting partners and regularly scanning digital domains for suspicious activity is not a novel idea: some might even call it "common sense". But it won't happen before organizations understand the scale of 3PC and the role it plays in their business. Until then, 3PC is a problem that influential tech vendors will exacerbate as long as they fail to talk about it.



THE AUTHOR

Chris Olson founded The Media Trust with Dave Crane in 2005. As CEO, he drives the company's vision, direction and growth plans. Prior to establishing The Media Trust, he spent four years as the chief operating officer and board member at Spheric Media. From 1998 until 2000, he was the vice president, global equities at Commerzbank; and from 1993 until 1998, he was the vice president of electronic trading at Salomon Brothers, Inc.

Olson currently serves on the board of the Interactive Advertising Bureau's Advertising Technology Council, as well as the Brand Safety Institute. He earned his bachelor's degree of science in finance from Georgetown University and a master's of business administration and a master's of science information systems from New York University's Stern School of Business.

CONNECT

linkedin.com/in/chris-olson

twitter.com/3pc_ChrisOlson

www.Digital3PC.com

703-893-0325