

Ongoing scam tricks kids playing Roblox and Fortnite

reader comments

13 with

Thousands of websites belonging to US government agencies, leading universities, and professional organizations have been hijacked over the last half decade and used to push scammy offers and promotions, new research has found. Many of these scams are aimed at children and attempt to trick them into downloading apps, malware, or submitting personal details in exchange for nonexistent rewards in *Fortnite* and *Roblox*.

For more than three years, security researcher Zach Edwards has been tracking these website hijackings and scams. He says the activity can be linked back to the activities of affiliate users of one advertising company. The US-registered company acts as a service that sends web traffic to a range of online advertisers, allowing individuals to sign up and use its systems. However, on any given day, Edwards, a senior manager of threat insights at Human Security, uncovers scores of .gov, .org, and .edu domains being compromised.

“This group is what I would consider to be the number one group at bulk compromising infrastructure across the Internet and hosting scams on it and other types of exploits,” Edwards says. The scale of the website compromises—which are ongoing—and the public nature of the scams makes them stand

out, the researcher says.

The schemes and ways people make money are complex, but each of the websites is hijacked in a similar way. Vulnerabilities or weaknesses in a website's backend, or its content management system, are exploited by attackers who upload malicious PDF files to the website. These documents, which Edwards calls "poison PDFs," are designed to show up in search engines and promote "free *Fortnite* skins," generators for *Roblox*'s in-game currency, or cheap streams of *Barbie*, *Oppenheimer*, and other popular films. The files are packed with words people may search for on these subjects.

Advertisement

When someone clicks the links in the poison PDFs, they can be pushed through multiple websites, which ultimately direct them to scam landing pages, says Edwards, who presented the findings at the Black Hat security conference in Las Vegas. There are "lots of landing pages that appear super targeted to children," he says.

For example, if you click the link in one PDF advertising free coins for an online game, you are directed to a website where it asks for your in-game username and operating system, before asking how many coins you would like for free. A pop-up appears saying, "Last Step!" This "locker page" claims the free game coins will be unlocked if you sign up for another service, enter personal details, or download an app. "I've tested it hundreds of times," Edwards says. He has never received a reward. When people are led through this maze of pages and end up downloading an app, entering personal details, or any number of required actions, those behind the scams can earn money.

These kinds of scams have been around for a while, ad fraud researchers say. But these stand out, as they all have links back to the advertising firm CPABuild and the members that work for its network, Edwards says. All the compromised

websites that have PDFs uploaded are calling to command-and-control servers owned by CPABuild, Edwards says. "They're pushing advertising campaigns into someone else's infrastructure," he says. Googling for a file linked to the PDFs brings up pages of results of compromised websites.

CPABuild's website, which lists its legal registry in Nevada, describes itself as a "content-locking network first and foremost." The company, which has existed since 2016, hosts tasks from its customers, such as giving people the chance to win money by submitting their email and postal code details. Then users of CPABuild, often known as affiliates, try to get people to complete these offers. They often do so via spamming links to YouTube comments or creating the kind of pop-up "locker" pages towards the end of the poison PDF click chain. This results-based process is known as a cost per action (CPA) by advertisers and marketers.

Advertisement

WIRED contacted multiple email addresses listed on CPABuild's website, as well as sending questions via a contact form, but we did not receive any response. The company website does not name any individuals who are behind CPABuild and is sparse on overall details. The website claims it has "daily" fraud checks in place to catch bad actors abusing its platform, and its terms of service prohibit those using it from being involved in fraud and from sharing multiple kinds of content.

The website claims it has paid out more than \$40 million to publishers and has thousands of templates and landing pages. Within CPABuild, there are various tiers of users. The website's affiliate structure is displayed in an image on its homepage. Members can be categorized as managers, devils, demons, wizards, masters, and knights. In one video uploaded by a CPABuild member on August 11, an admin account can be seen sharing a message with users that indicates the company has taken steps to prevent the platform from being used for fraud. "We are still getting reports that CPABuild publishers

are promoting offers in ways that violate our terms of service,” a message seen on the screen reads. Edwards’ research shows, however, that whatever efforts CPABuild has taken have failed to prevent its users from engaging in rampant fraud.

“CPA fraud, which includes cost per app install, is very common,” says Augustine Fou, an independent cybersecurity and ad fraud investigator, who reviewed a summary of Edwards’ findings. “Specialists like the ones identified in the research carve out a niche where they become the category leader in a particular kind of fraud,” Fou says. “Customers come to them for that speciality.”

Scores of websites are currently impacted by the PDFs. This week, the New York State Department of Financial Services removed PDFs uploaded after being contacted by WIRED. Ciara Marangas, a spokesperson for the department, says the issue was first identified in 2022, and following a review and additional steps, the files were removed.

<https://arstechnica.com/?p=1961085>