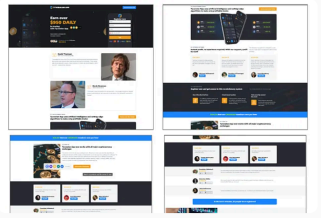
Page not found

Latest Top

Tracking Software Weaponized by Criminals

Inside four months of joint research with Infoblox Threat Intel on the abuse of Keitaro Software.

MAR 24 • CONFIANT



Analyzing a Live AiTM Attack Targeting Google Accounts via Malvertising

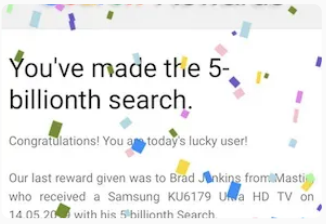
We captured a malvertising campaign delivering an Adversary-in-the-Middle (AiTM) kit. Here, we unpack a paradox— an…

PUBLISHED ON ROSHAN • MAR 24

Malvertiser “D-Shortiez” abuses WebKit back button hijack in forced-redirect campaign

Over the last few years, as AdTech and browser security has continued to mature, many malvertisers have moved on from…

MAR 2 • CONFIANT AND ELIYA STEIN

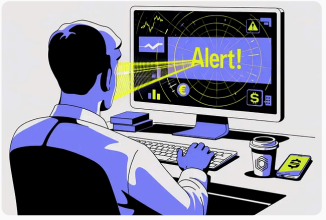


FEBRUARY 2026

Disrupting 59M Malicious Impressions: Inside D-Shortiez Testing Infrastructure and Campaign Management

Two clusters, one password, and the automated harvesting that blocked campaigns before deployment

FEB 24 • CONFIANT AND MICHAEL STEELE



The Curious Case Of MutantBedrog's Trusted-Types CSP Bypass

MutantBedrog is a malvertiser that caught our attention early summer '24 for their highly disruptive forced redirect campaig…

How One "Crypto Drainer" Template Facilitates Tens Of Millions Of Dollars In Theft

FEB 3 • CONFIANT AND ELIYA STEIN

Crypto Drainers are phishing pages that lure victims into signing malicious transactions that allow the attacker to siphon their…

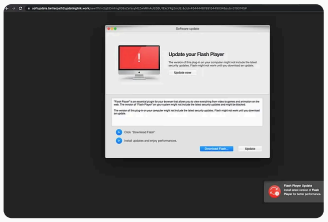
FEB 3 • CONFIANT AND ELIYA STEIN

A Whirlwind Tour Of Crypto Phishing

The post-pandemic world has seen cryptocurrencies and blockchain products in general catapult in valuation and…

FEB 3 • CONFIANT AND ELIYA STEIN

How File Hashes Fail As A Malware Detection Heuristic



In this blog post we take a trip downstream from malvertising delivery mechanisms and take a close up look at a fake Flash…

FEB 3 • CONFIANT AND ELIYA STEIN

Profiling hackers using the Malvertising Attack Matrix by Confiant

A relatively new threat vector, Malvertising is a cyber-attack relying on ad networks and digital ads exposing virtually any…

FEB 3 • CONFIANT

Looking At Chrome Extensions That Hijack Search - Spread Via Malvertising

In this blog post we discuss an ongoing malvertising campaign

The Trend Of Client-Side Fingerprinting In Cloaked Landing Pages

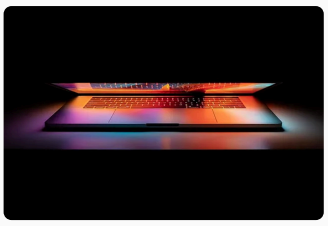
This blog post will examine the client-side aspect of cloaking in non auto-redirect based malvertising chains.

FEB 3 • CONFIANT AND ELIYA STEIN

Malvertising, Site Compromise, And A Status Report On Drive-by Downloads

This blog post will explore the details behind a recent spree of website hacks and the malicious payloads that were embedde…

FEB 3 • CONFIANT AND ELIYA STEIN



Exploring The Impact Of Malvertising On Government, ISPs & The Fortune 100

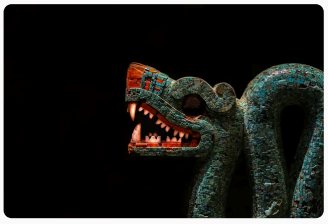
In this blog post we will explore the threat of malvertising from the other end of the tunnel and look at what organizations are…

FEB 3 • CONFIANT AND ELIYA STEIN

New macOS Bundlore Loader Analysis

Looking at a recent Malvertising campaign detected by Confiant's realtime Malvertising detection engine, we stumble…

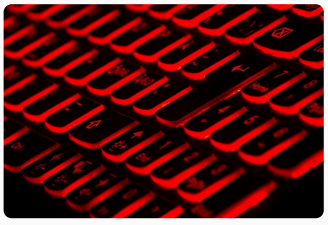
FEB 3 • CONFIANT



Malvertiser 'eGobbler' Exploits Chrome & WebKit Bugs, Infects Over 1 Billion Ads

Over the past 6 months, the threat group has leveraged obscure browser bugs in order to engineer bypasses for built-in browse…

FEB 3 • CONFIANT AND ELIYA STEIN

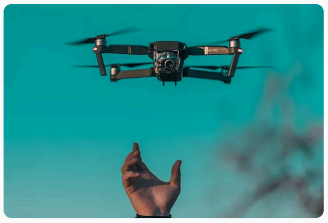


Revealing How "The Dandelion Group" Leverages

How Malvertisers Weaponize Device Fingerprinting

HTTP cookies are utilized to keep a local record of visitors' browsing activity in order to personalize the web surfing…

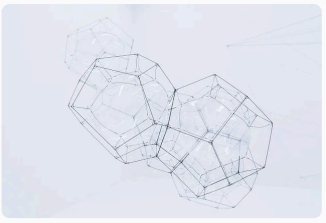
FEB 2 • CONFIANT AND ELIYA STEIN



The Malvertising Campaign Lifecycle

This blog post is an investigation into the typical lifecycle of resources that serve malicious display ads, or as we like to c…

FEB 2 • CONFIANT AND ELIYA STEIN

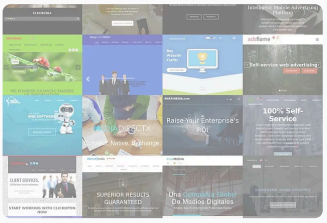


JANUARY 2026

Uncovering 2017's Largest Malvertising Operation

The Zirconium group successfully created and operated 28 fake ad agencies to distribute malvertising campaigns through 201…

JAN 30 • CONFIANT



Hands On With Malvertisers' Sneaky Tricks

These days when we talk about digital ad fraud, most of us in Ad Tech think immediately about non-human traffic or nefariou…

JAN 29 • CONFIANT AND ELIYA STEIN

How Bad Ads Hijack Your Browser With One Simple Trick

Forced mobile redirects are perhaps the most pervasive ad security concern today for both publishers and consumers of…

JAN 29 • CONFIANT AND ELIYA STEIN

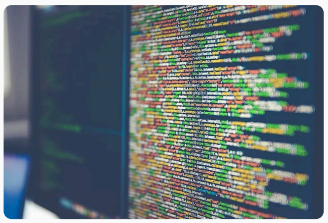
Phantom Stores: Retail Impersonation Spreads Ahead of Black Friday Powered by Video Ads and Modular 'Holiday Skins' Kit

In the frenzied weeks leading up to Black Friday and Cyber Monday, Ad Tech's busiest season, a new cluster of phantom…

NOV 24, 2025 • CONFIANT AND ROSHAN

SEPTEMBER 2023

Exploring ScamClub Payloads via Deobfuscation Using Abstract Syntax Trees



ScamClub is a prolific threat actor in the programmatic ad space known to carry out large-scale attacks with the purpose of…

SEP 27, 2023 • CONFIANT

JUNE 2022

How SeaFlower 藏海花 installs backdoors in iOS/Android web3 wallets to steal your seed phrase

During the course of our work at Confiant, we see malicious activity on a daily basis.

JUN 12, 2022 • CONFIANT