Today’s ad networks

There are a variety of delivery methods for online advertising, though ad exchanges are one of the most common today. This process includes publishers who post the ads to the site, exchanges that facilitate bidding for ad placement, and advertisers who bid to win placement on the site.

This process is similar to a car auction. The seller (web user) puts their car (ad space) up for sale at an auction house (publisher). The auctioneer (ad exchange) opens bidding to potential buyers (advertisers). The highest bid wins and the buyer pays the user with money (ad).

The data that drives the process—determining which ads advertisers bid for and how much they bid—is the information gathered about the user. Geographic location, language, browser type and version, and operating system can commonly be determined when a page loads.

B“ad” actors

The bar is quite low in terms of who qualifies as an “advertiser.” In many ways this is necessary for smaller sellers to get their ads easily distributed. However, it also leaves the door open for bad actors.

Without significant vetting on many advertising networks, it’s fairly straightforward for cyber criminals to enter these networks and bid for ad placement alongside legitimate advertisers.
How malvertising works

A bad actor usually can’t send a user directly to a page with an exploit or malicious payload without being found out.

As a result, attackers leverage redirection. When a redirection is included, the browser is told to go to another site to retrieve the content it is looking for.

Using this method, an attacker can attempt to distribute any sort of payload they wish. In many cases, the final content displaying on the user’s page is an ad that entices them to download adware or PUAs.

In other cases, the malicious ad opens a window or alert that attempts to trick the user into thinking if they attempt to install the fake update, they find themselves infected with malware.

However, what’s most concerning is the information that an attacker can glean from a user can be used for active exploitation. For instance, an attacker can choose to only bid on ads that come from users running Internet Explorer.

Obtaining the winning bid, the attacker can send an Adobe Flash Player exploit in their “ad.” If the version of Flash installed is out-of-date, the machine can be compromised without the user even clicking the ad.

The attacker has exploited the browser right out of the gate, requiring zero interaction from the user apart from loading the page that contains the ad.

### Cisco Umbrella
- Domain-level protections will help to block redirects to domains that are known to be malicious, often stopping a series of redirects halfway through the chain.

### AMP for Endpoints
- An endpoint protection application can prevent malicious payloads from being installed onto a computer that encounters a malicious advertisement.

### Secure Internet Gateway/Web Security Appliance
- Cisco’s Secure Internet Gateway and Web Security Appliances contain web scanning features that can prevent access to malicious websites.

### Next-Generation Intrusion Prevention System
- Network Security appliances that include IPS signatures can detect malicious activity such as exploit attempts against vulnerable software.