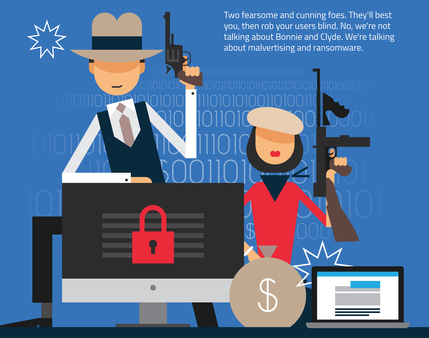
# MALVERTISING AND RANSOMWARE

## The Bonnie and Clyde of advanced threats



Two fearsome and cunning foes. They'll best you, then rob your users blind. No, we're not talking about Bonnie and Clyde. We're talking about malvertising and ransomware.

### Malvertising

Malicious advertising, or the use of online advertising to distribute malware with little to no user interaction required.

### Ransomware

Malware that will encrypt or lock data files, and then demand a ransom payment to decrypt or unlock them.

**70%**

The estimated amount of malvertising campaigns that deliver ransomware as a payload.

Malvertising is the unseen enemy delivering one of the most dangerous forms of malware today—ransomware. It hits your users without their knowledge, often hidden on reputable sites. When it strikes, it turns common software programs against your users to infect machines.

## Malvertising's public enemy era

**2007**
Malvertising first noticed on Myspace and Rhapsody using Adobe Flash

**2009**
A click-fraud scam runs on NYTimes.com

**2011**
Malvertising increases 2.5x over the previous year. Ads on Spotify serve malware that doesn't need users to click

**2012**
LATimes.com hit with massive malvertising attack using the Blackhole exploit kit

**2013**
A campaign targeting Yahoo! infects machines with Banker Trojans

**2014**
Google disables more than 524 million bad ads and bans thousands of advertisers

**2015**
Malvertising in just the first half of 2015 increases 260% compared against all of 2014*

**2016**
Large Angler malvertising campaign hits top publishers, spreads ransomware

*RiskIQ

## Malvertising appears on highly trafficked sites

In March 2016, top websites were hit with banner ads that attempted to install ransomware.

| Websites | Monthly traffic* |
|---|---|
| msn.com | 1.3B |
| nytimes.com | 313.1M |
| bbc.com | 290.6M |
| aol.com | 218.6M |
| nfl.com | 60.7M |
| realtor.com | 51.1M |

If your users were visiting these sites to conduct research during business hours, they could have been hit with a "drive-by-download," which doesn't require them to click on infected ads to start the attack chain.

*Similarweb.com

## How they git ya

### How online advertising works

1. Advertisers sign up with an advertising network
2. Advertisers bid to have their ads appear on popular websites
3. Billions of ads are shown to users and targeted to their profiles in real time

### How criminals slip by ad networks

1. Buying advertising space is increasingly being transacted automatically
2. Not all advertising networks have strict criteria for advertisers
3. Bad actors will serve good ads for a while before switching to ads that deliver ransomware

### How malvertising delivers ransomware

1. The infected ad uses an iframe (invisible webpage element) to redirect to a landing page
2. Malicious code attacks the user's system from the landing page via exploit kit
3. The exploit kit installs ransomware

## Don't get squeezed

New malvertising techniques exploit security loopholes.

### Are you running security software that detects fingerprinting?

Malvertising uses fingerprinting to detect when a computer is running on a virtual environment or is using advanced security products. It will not serve its payload to those computers to avoid being detected.

Some security products can detect when fingerprinting is being used and flag it as suspicious.

**So now malvertising is camouflaging its fingerprinting techniques.**

### Do your machines run Adobe Flash?

Flash renders graphics and animation and is heavily used by the ad industry. Flash's zero-day vulnerabilities allow for exploit kits to load when the ads load.

Unpatched Flash software on endpoints will increase exposure to malvertising and ransomware.

**In 2015, 314 vulnerabilities were found in Adobe Flash. That's up from 76 in 2014.***

*CVE Details

## Watch yer back

### Protect against malvertising

- Train your staff on good security practices
- Keep your software patched and remove software you don't use
- Run the latest browsers and effective anti-exploit software

### Protect against ransomware

- Back up files to a highly-encrypted cloud service with multi-factor authentication
- Delete encrypted files from backup history
- Layer security with an effective anti-exploit program, in addition to firewall, antivirus, and anti-malware software

To protect your business from the Bonnie and Clyde of cybercrime, go to **malwarebytes.com/business.**

Malwarebytes