PUBLISHERS & MALWARE:
ARE YOU AT RISK?

Presented by geoedge

Powered by DIGIDAY CONTENT STUDIO

PUBLISHERS & MALWARE: ARE YOU AT RISK?

Malware is more than just a catchy combination of "malicious software." These programs, plug-ins and pieces of code are designed to damage, disable and take over computers and networks. Malware is a global scourge that costs businesses an estimated $114 billion annually.

Publishers are especially at risk.

Among the most common forms of malware is adware — unwanted software that's automatically displayed or downloaded via advertising material. (See our "Malware Glossary" on p. 9 for other terms you must know.) Adware is a particular problem for publishers. Imagine if simply thumbing through a newspaper infected the reader with the flu and then drained his bank account.

To protect their users — and their own brands — publishers must prevent malware attacks from being launched through their websites and apps. Working with Digiday Content Studio, GeoEdge produced this booklet to help you make sense of this dangerous landscape and determine what threats you're facing.

On page 3, we document two recent malvertising attacks on publishers, and explain how they were carried on. Then, test your knowledge on page 6 with "The Truth About Malware." Finally, on page 22, we present our "Best Practices for Publishers Defending Against Malware," including advice on how to handle a breach.

If you'd like to discuss your malware-protection strategy, please request a consultation at **geoedge.com**.

A TALE OF TWO MALVERTISING ATTACKS

What do the *Huffington Post*, *GameZone*, *The Jerusalem Post* and *LA Weekly* have in common?

They've all fallen victim to recent malvertising attacks.

January 2015: Advertising.com spreads ransomware

A few days into the new year, Advertising.com was compromised by malware. As a result, the popular ad server (owned by AOL) distributed dangerous malware to a number of high-profile, high-traffic publishers, including *The Huffington Post*, *GameZone* and *LA Weekly*.

The payload was the very aggressive Kovet ransomware, which prevented users from accessing their mouse and keyboard until a ransom was paid. According to CSO, AOL's network delivers ads to a staggering 199 million uniques every month in the U.S. alone. (That's about 90% of the entire American Internet audience.) Even if just a tiny percentage of affected users paid the ransom, the hackers earned a sizeable if ill-gotten paycheck.

Though they were called out by reporters covering the breach, the publishers were not really at fault. The malvertising was technically delivered via AOL's ad servers; most likely, it had passed security screening by masquerading as legitimate code. Upon activation, the hidden malware redirected users to a number of different websites, with each step disguising both the code's source and its true purpose. Eventually, the ransomware was unleashed and remained active for two days.

This is more common than you might think, and malvertising does not discriminate. In the AOL assault, the other victims included *FHM*, a men's lifestyle magazine and website and Soap Central, a community for soap opera fans.

Despite assurances from networks that they screen every ad, malvertising is sneaking past these figurative guard towers. Publishers themselves must step up prevention efforts.

September 2014: Cryptowall takes over DoubleClick

The AOL attack was hardly the first of its kind. Five months earlier, Google's DoubleClick network fell victim to a similar attack. In this case, the infamous ransomware Cryptowall was distributed by several well-known publishers, including *The Times of Israel* and *The Jerusalem Post*.

This attack illustrates the dynamic nature of malware. By presenting itself as harmless code during initial scans, malware can bypass rudimentary security measures. In reality, the damaging code can be activated at a later time. The trigger can be based on any number of variables. For example, the code may be harmless at 8 a.m. for users in France; then, four hours later, readers with Canadian IP addresses find themselves targeted by a malvertising attack.

In the worst cases, these visitors don't even know they're infected. The code may hijack your traffic through domain spoofing; it may run a "traffic fraud" campaign; it may even insert illegitimate ads into your inventory. Even when publishers have their own server protection measures in place, third-party ads can still reach users because they're coming from external servers.

In the DoubleClick attack, the financial damage cannot be determined because it's impossible to know how many ransoms were paid.

Likewise, brand damage is impossible to enumerate. You, as a publisher, should be aware of the risks and take back control.

THE TRUTH ABOUT MALWARE

It's a popular topic, but misunderstandings persist, even among publishers who have been defending against malware for years.

Test your malware knowledge with this short quiz.

Malware is only a threat to visitors of less reputable websites.

FALSE

Malware attacks are no longer associated with pirating and pornography. Virtually all consumer-facing websites are vulnerable to attack, even those that require user registration and identity verification.

Malware only affects desktop computers and browsers.

FALSE

Mobile malware is on the rise, and some experts believe attacks on smartphones and tablets are poised to increase. With so much personal information being stored in our pockets, mobile targets are irresistible for hackers and criminal organizations. As more publishers revamp their websites for this "mobile-first" world, ad verification is critical to preventing attacks.

Publishers are protected when ad servers offer malware protection.

FALSE

Even when a publisher's ad server provides malware protection (eg, Google's DoubleClick for Publishers), the ad server can only scan campaigns that are directly delivered via that platform. When the initial tag directs the user browser to a third party, from that point going forward the publisher's ad server is not part of the delivery chain — and therefore cannot screen for malware.

Ad servers and exchanges are held responsible for malware served through their assets.

FALSE

While some partners may accept responsibility in terms of campaign costs, publishers are ultimately on the hook for lost revenue — and, most importantly, for brand damage caused by a compromised user experience.

Malware can't infect premium campaigns that are served directly by publishers.

FALSE

Even advertising assets that pass initial verification can be compromised, sometimes triggered to serve malware at a later date, to a specific geographic region or to a specific audience. Ongoing ad verification is critical to prevent such "sleeper" attack.

Malware is always downloaded and can't affect on-site user experience.

FALSE

Not all malware is designed to compromise computers. For example, when deployed as malvertising, malware can hijack advertising inventory, replacing paid placements with unauthorized assets. In some cases, publishers may never even know it's occurring. Only the users, whose experience has been compromised, will be harmed.

KNOW YOUR MALWARE

Everyone recognizes malware as a program, plug-in or other piece of code designed to damage, disable or take over a computer or network.

But do you also know about **cookie stuffing**, **MITM attacks**, **scareware** and the other lesser-known threats that malware poses to your users?

Turn the page to learn more.

A

Ad Verification Service

Typically a third party, these service providers scan creative assets and targeted landing pages to identify malware, malicious activities and other inappropriate campaigns. For publishers, an ad verification service plays a critical role in malware protection, particularly for ongoing campaigns that can be susceptible to corruption.

Adware

In its most innocent form, adware is any code designed to insert advertisements onto websites, apps or software packages in order to drive revenue through page views, downloads or other conversions. In worse cases, on publisher websites, adware can interrupt and harm the user's experience and may even hide destructive malware.

Auto Download

The process of forcing a user to download unwanted software to their computer or mobile device. With malicious adware or Malvertising, the software can force out or replace legitimate advertising assets.

Auto Redirect

Also known as "browser hijacking," the process of taking over a user's web browser for the purpose of misdirecting that user to another site without their knowledge or permission. In some cases, interstitial ads will prompt user engagement, which may grant system permission to the malware.

Auto Refresh

Commonly associated with fraudulent CPM activity — where the advertiser is paying per impression — auto-refresh hacks compromise user experience by interrupting site visits and app sessions.

B

Backdoor

A method for bypassing normal security and authentication routines, often used by programmers during development to save time. When left in place, backdoors can create serious vulnerabilities for publishers who run their websites using "off-the-shelf" software.

Bot

Short for "robot," a bot is a program that simulates human activity. Bots can be used by criminals to uncover vulnerabilities on individual and network computer systems — and then install malicious software. A computer that's been hijacked by malware may become a bot (sometimes also called a "zombie") and put to criminal use.

Botnet

A collection of bots, coordinated by a central system to execute functions that require large amounts of computing power. An individual computer owner may have no idea that his or her computer is part of a botnet.

C

"Contains Malware"

A common warning that malware has been discovered on a particular website or app. Knowing that "Contains No Malware" is increasingly difficult to guarantee, many publishers rely instead on disclaimers in their Terms of Service, stating that they've done their best to provide a risk-free user experience and cannot be held responsible for damages.

Cookie Stuffing

Also known as "cookie dropping", the practice of providing a client with falsified cookies to give the impression that a user had visited other domains. This is a common trick to defraud affiliate advertising programs.

D

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

Techniques vary, but the most common DoS/DDoS attacks involve flooding the victim's servers with an unmanageable amount of requests, causing them to overload and essentially shut down. Malware-infected Botnets are typically used to carry out these attacks without the owner's knowledge.

Droneware

A specific kind of malware used to take remote control of a user's computer and, typically, add it to a Botnet.

E

Embedding

The act of including unwanted malware alongside legitimate software.

Exploit

The general term for any attack on a computer system or software. The term's origins point to the fact that most attacks take advantage of vulnerabilities, rather than relying on so-called "brute force," which overpowers security systems.

F

Firewall

A protective barrier placed between internal and external systems, software and users.

G

Grayware

As the name implies, software that walks the line between being legitimate and nefarious. For example, unwanted Adware that does nothing more than display pop-up ads might be considered grayware. Some publishers may have a greater tolerance for grayware appearing in their inventory.

H

Hidden Ads

Ads placed in such a manner that they are never viewable. For example, stacked ads, ads clipped by iframes and zero-opacity ads.

Host File

A file containing the names and IP addresses of other computing systems, including websites. Hackers can Spoof a host file, opening the victim's computer to attack.

K

Keylogger

Software that records keystrokes to covertly capture a user's password and other credentials (see also Spyware).

M

Macro Virus

Malicious software built specifically inside a specific program. In the 1990s, Microsoft Excel was famously infected by macro viruses that were passed along unknowingly within spreadsheets.

Malvertising

The use of online advertising to spread malware.

Man-in-the-Browser (MITB) and Man-in-the-Middle (MITM) Attacks

By inserting themselves into a transaction without detection, MITB and MITM attackers intercept sensitive data — but typically allow the transaction to continue. For example, a hacker might sit "in the middle" of a bank transfer, collecting the user's account information; the transfer is not actually interrupted, leaving the attacker undetected.

P

Personally Identifiable Information (PII)

A legal term that can include an individual's name, birth date, Social Security number, account numbers, email address and so forth. Gathered by malware, PII is traded openly on the black market, with the most sensitive data commanding the highest prices. Even seemingly innocuous personal details, such as those gathered by many publishers, can gain value when paired with data stolen from other sites.

Pharming

A form of phishing, pharmers redirect unsuspecting users to a malicious website, often by spoofing the legitimate destination. The purpose can be stealing PII, installing malware or adding the victim's computer to a Botnet.

Phishing

One of the oldest tricks in the malware book, phishing is acquiring sensitive details by masquerading as a trusted authority. Publishers are particularly vulnerable to phishing attacks on their subscribers, who may reflexively trust an email that looks legitimate at a quick glance.

Plug-In

A small piece of software installed within a larger program, often to add functionality. Installing plug-ins recklessly, without confirming their origins, is a popular cause of malware intrusions. Publisher platforms, such as WordPress, rely heavily on plug-ins and must be continuously monitored for malware attacks.

Port Scanning

Using software designed specifically for locations (or "ports") on servers and individual computers, malware can find vulnerabilities before IT has time to install a patch.

Potentially Unwanted Application (PUA) and Potentially Unwanted Program (PUP)

Related to Grayware, PUAs and PUPs are applications, programs or plug-ins that may be relatively harmless, like Adware, or may hide destructive code such as a Virus or Worm.

R

Ransomware

A popular new form of malware that takes control of a user's files, computer or server, then demands payment to release the data or controls. Ransomware has gained popularity in part due to Bitcoin, which makes it possible to receive ransom payments anonymously.

Root-Level Access

The Holy Grail for hackers, root access gives the user supreme authority on a computer or network. In other words, they have total control and impunity to install malware.

Rootkit

Software used by hackers to gain root-level access.

S

Scareware

Typically masquerading as adware, scareware is designed to frighten users into believing their systems are vulnerable, prompting them to install a solution. The new installation, of course, is the true malware.

Social Engineering

The spycraft of hacking, social engineering is the process of impersonating an individual to gain access to sensitive information. Often, hackers use one part of an individual's personal details to gain access to more data. For example: using part of a stolen Social Security number to reset a Gmail password, then using that Gmail account to reset a bank account password. Malware is used to automate part of the process: By posing as a friend on a social network, for example, malware can prompt a victim to divulge sensitive information.

Spoofing

The act of falsely representing a known website, service or email address in the hopes of prompting users to install malware or divulge sensitive personal data.

Spyware

Software that gathers personal or organizational details without the user's knowledge or consent.

T

Trojan Virus

Named for the Trojan Horse in Virgil's "Aeneid," these viruses appear to be innocent but actually conceal dangerous malware. Unlike worms and traditional viruses, Trojans don't spread on their own — they trick users into installing them. Once in place, they can download even more malware, steal personal information or turn over Root-Level Access to hackers.

V

Virus

A software, plug-in or other type of code designed to wreak havoc on a computer, typically by attaching itself to existing software.

W

Worm

Related to viruses, worms are also designed to duplicate and distribute themselves across a system or network. Unlike viruses, which are attached to specific software, worms are generally standalone, relying instead on vulnerabilities to spread.

Z

Zero-Day Exploit

A vulnerability that's completely unknown to the software programmer or vendor, presenting a brief breach window (the so-named "zero day") during which malware can Exploit a system.

RISK ASSESSMENT FOR PUBLISHERS

As they say, the best offense is a good defense.

Answer these 10 questions to get a better handle on your exposure to malware.

RISK ASSESSMENT FOR PUBLISHERS

1. What is your monthly traffic?
2. How much, if any, third-party code is regularly hosted on your website?
3. How many ad sources (eg, agencies, premium advertisers, third-party) do you engage in any given month?
4. How many new ad partners do you approve each month?
5. How much control do you have over your own ad server? For example, do you host everything on your own servers or with a third party?
6. Do you have full, partial or minimal access or transparency to assets served to your inventory?
7. What is your tolerance when it comes to malware?
8. What, if any, are your regulatory and legal liabilities when it comes to malware attacks?
9. Do you have exposure to app store malware policies? If so, are you confident in your compliance?
10. In the event of a breach, do you have a plan in place?

To learn how your answers to these questions can impact your brand's reputation, please contact **GeoEdge** for a free consulation.

BEST PRACTICES FOR PUBLISHERS DEFENDING AGAINST MALWARE

No one wakes up saying, "Today I plan to get hacked."
Bad things can happen at any time.

Are you prepared?

PROTECT YOURSELF (AND YOUR USERS)

1. Define your malware policies and action plan in advance. Considering the prevalence of so-called "grayware"—which walks the line between legitimate code and malicious software—it's not enough to just say "no malware is allowed."

2. Educate yourself on malware as it relates to publishers, and dedicate enough resources to remain current on the latest news and alerts from the security industry.

3. To the greatest degree possible, vet your buyers and advertisers before accepting their assets on your site or app. In your partner agreement, spell out penalties in the event of a policy breach.

4. For direct campaigns
   Scan all creative and landing pages from different geographic locations and using different target parameters before uploading them to your ad server.

   Perform daily checks for compliance breaches in your advertising assets that have been previously approved. Continue this during their entire run within your inventory.

   For third-party campaigns
   Constantly scan all live campaigns (both creative and landing pages) that are served within your inventory.

5. Ensure that your ad verification service will notify you in real-time when malware or other malicious activities are detected within your inventory.

IF MALWARE IS DETECTED

1. Identify the specific creative or campaign(s) where the malware has originated.

2. Gather as much information as possible of the incident and whom it is targeting.

3. Pinpoint the "bad" mediator.

4. Block the campaign immediately.

5. Inform the channel.

GeoEdge is the premier provider of ad verification and transparency solutions for the online and mobile advertising ecosystem. The company ensures high ad quality and verifies that sites and apps offer a clean, safe and engaging user experience. GeoEdge guards against non-compliance, malware, inappropriate content, data leakage, operational and performance issues.

Leading publishers, ad platforms, exchanges and networks rely on GeoEdge's automated ad verification solutions to monitor and protect their ad inventory.

To find out how GeoEdge can enhance your quality assurance and verify your online and mobile campaigns, head to **www.geoedge.com.**