See. Control. Secure.

Threat Bulletin

Adware

January 2020

Introduction

"If you're not paying for something, you're not the customer, you're the product being sold."

Internet wisdom

Most cybercrime is driven by money. From building botnets to stealing banking credentials, perpetrating click fraud, or ransoming files, money is the goal. Criminals are always looking for ways to maximize their income, shifting their tactics in response to market trends. For cybercriminals, one of the most common and lucrative means of generating revenue is adware.

Did you ever encounter pop-up ads in weird places, or an unusually high frequency of distracting advertisements? Chances are, you encountered a malicious version of adware — unwanted software designed to aggressively display ad content, sometimes at the expense of legitimate ads.

Adware (short for "advertising-supported software") is not a highly sophisticated cyberattack, but in fact, it's the malware type you're most likely to encounter in your daily digital life. It's ranked as the most prevalent type of consumer malware, regularly infecting tens of millions, or even hundreds of millions of devices at a time. What is dangerous about adware is that it opens the door for cybercriminals to potentially add other malicious functionality, which could be far more serious. It can also come bundled with other types of malware, foreshadowing worse cyberattacks to come.

What is Adware?

It's important to differentiate between adware as a business model in software development and malicious adware. Legitimate free services and programs usually make money by using online advertising, with ads typically bundled within the program and displayed in ways the program developer specified. Adware in this sense is the 'price' for enjoying the free content. If you're not paying for something, get ready to watch the ads – as you're the product being sold.

While this advertising model is a common and a legitimate way to make money, cybercriminals found the way to abuse this scheme for their benefit. With malicious adware, unwitting users download it without realizing its real intent – in many cases it hides inside legitimate programs. This type of adware displays multiple unwanted advertisements that do not come from sites the user is visiting. It can also redirect users' search requests to advertising websites, collect data, and serve malicious activity, such as click fraud, to users.

Today, the volume of adware is on the rise thanks, in part, to the proliferation of mobile devices. Adware is making its way into more and more mobile apps. Cybercriminals are using more aggressive techniques than simply hijacking, including hiding within Trojans, bundling with ad fraud components, or demonstrating rootkit capability, which makes the malware difficult to remove. Additionally, many adware strains implement various stealth and resilience techniques to stay hidden on the device as long as possible.

At their most innocuous, adware infections are just annoying. Multiple pop-up ads can slow down your Internet experience and make your computer more prone to crashing. More important are the privacy issues that adware creates – personal data can be stolen and traded. Also, the advertising industry suffers real damage – it pays for fraudulent clicks, and websites lose ad revenue.

Adware continues to dominate the threat landscape as it is a fairly safe means of monetization for the criminal. Adware is typically built into freeware or shareware programs users download from the internet - it forms an indirect 'price' for using the free program. On mobile, cybercriminals distribute apps with adware through third-party app stores for Android, and even sneak adware-laced apps into official app stores, such as the Google Play Store or Apple's App Store.

Google tracks more than 60 million attempted adware installs per week, which are three times the number of other malware attempts combined. Why is adware is so prevalent? First of all, because it is very simple. It doesn't require any elaborate hacking techniques. It isn't trying to steal your money. The revenue generated by ads is what draws adware to your PC or mobile device. Advertisers often pay out based on impressions, i.e. the number of people who view the ads. Scammers have realized that the more ads they can rain down on their victims, the more money they can make.

Stealth Techniques

Typically, to achieve persistence, adware uses various stealth techniques to hide its presence on the affected device:

- The app loaded with adware hides its icon and creates a shortcut instead. If a typical user tries to get rid of the malicious app, chances are that only the shortcut ends up getting removed. The app then continues to run in the background without the user's knowledge.
- If the user wants to check which app is responsible for the ad being displayed, by hitting the "Recent apps" button, another trick is used: the app displays a Facebook or Google icon. The adware mimics these two apps to look legitimate and avoid suspicion – and thus stay on the affected device for as long as possible.

Business Model

Adware is a highly lucrative business. Let's take a look at how the adware economy works.

Advertisers (either directly or through brokers) pay money for ad views or clicks. Distributors get the adware on people's machines, usually by delivering it bundled with legitimate programs. When users install the package, they get the desired piece of software and a bunch of unwanted programs hiding alongside it, as well. The more things that get installed on an end user's phone or PC, the more the criminals get.

If you've ever downloaded a screen saver or other similar feature for your laptop, you've seen a 'terms and conditions' page pop up where you agree to the installation. Buried in the text that nobody reads is information about the bundle of unwanted software programs in the package you're about to download. That consent form is what allows the businesses making adware to operate legally.

These businesses operate through a network of affiliates **-** brokers who bundle advertisements (often unwanted software) with popular software, then place download offers on well-trafficked sites in which they're likely to receive clicks. Parties are paid separately - some legitimate developers do not even know their products are being bundled with unwanted software.

Once adware gets installed on a user's machine, it generates revenue in two ways: by automatically displaying online advertisements to a user, and through a per-click payment made when a user clicks on the ad.

Infection Methods

There are two main ways you can get infected by adware:

- **Via freeware**

The most common infection method is via the download of a free program. You download a program — usually freeware or shareware — and it quietly installs adware without your knowledge, or permission. Today, even paid software from an untrustworthy source can deliver an adware payload.

- **Via infected website (drive-by download)**

A site you're visiting can be infected with adware, which takes advantage of a vulnerability in your web browser to deliver a drive-by download. After it burrows in, the adware starts collecting your information, redirecting you to malicious websites, and throwing more advertisements into your browser.

What Adware Does

The scale of the damage that adware can do can range from quite innocent but annoying ads ("yellow level") to serious malware infection ("black level").

Yellow level

- Adware shows you intrusive ads (banners/pop-ups) that do not come from the websites you are visiting, including scam ads that recommend fake updates or other fake software;
- Turns random web page text into hyperlinks.

Red level

- Monitors your behavior online and gathers personal data about you so it can target you with customized ads;
- Modifies Internet browser settings without your knowledge or consent - adware programs that work in this way are often called browser hijackers. You might experience new tabs opening, a change in your home page or default search engine, or even a redirect to a malicious website.

Black level

- Wastes the device's battery resources;
- Generates increased network traffic – you might experience a slow Internet connection;
- Adware might use more intrusive methods and infect you with more dangerous malware, such as spyware, banking Trojans, bots, etc. This is the case with the "Pusher" adware family.

How to Protect

There are a few effective tactics that can be used to address different aspects of malicious adware.

- To check if your device is infected, download a reputable adware scanner from antivirus companies like Bitdefender, Malwarebytes, or Avast (it is usually included in all adware removal tools). But be careful to download the real program — adware and other malware tends to hide in apps that pretend to be adware scanners.
- Use an ad blocker: in many cases, a free service can be used without viewing ads. Ad blockers prevent ads from being displayed in a browser, eliminating the chance of clicking on something malicious while preventing drive-by downloads.
- Avoid using any third-party app stores, although even Google Play has been a source of adware-infested apps. Use only official app stores to download software and stick to prominent mainstream apps as much as possible. Always double-check what you're actually downloading, e.g. the real Twitter app, and not Twltter.
- Buy devices from trusted companies with reputable, built-in security: there have been numerous incidents in which people who purchased low-cost Android devices learned that adware was installed in core files.
- To combat the variety of threats out there, many telecom companies using the latest available technologies, like Vodafone, Telefonica, and Hutchison Drei, are turning to network-based security to protect customers. Check if your telecom operator offers a cybersecurity service that protects you on mobile and Wi-Fi networks by blocking various online threats, including adware.
- Ensure that your browser, operating system, and software have the latest updates and security patches. For example, Google is continuously tracking web pages known to host unwanted software offers and regularly updates the Safe Browsing protection in its Chrome browser to warn users when they visit such pages.

Conclusion

With revenue in the global digital advertising market predicted to hit $664.7 billion by 2026, there's no chance hackers will stop abusing adware for their benefit. By its nature, the whole ad industry is very vulnerable and prone to different kinds of online scams and cybercrime. Ad fraud, ad stacking, spoofing, malvertising, and ad injection are just some of the techniques on the continually expanding list. Malicious adware generates easy revenue for cybercriminals – at the expense of legitimate ads and user privacy. Malicious adware makes money by violating privacy and extracting lots of data about users — and then selling that data to third parties or using it for targeted advertising. To protect the privacy and security of consumers, CSPs can offer their customers network-based Security as a Service (SECaaS) such as NetworkSecure from Allot, which blocks popular online threats, including adware, and protects over 23 million subscribers worldwide.

Want to learn more about Security as a Service?
We can assist.

Contact Allot.