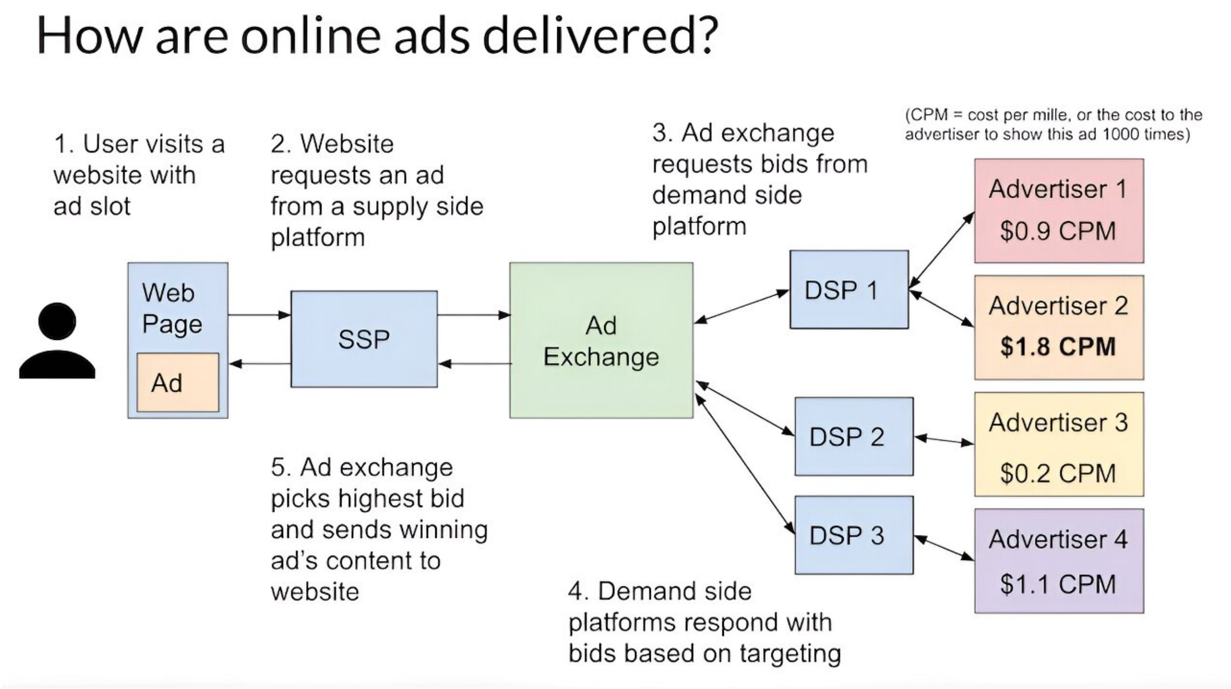
Spyware can infect your phone or computer via the ads you see online—report

September 22 2023, by Claire Seungeun Lee


How are online ads delivered?
1. User visits a website with ad slot
2. Website requests an ad from a supply side platform
3. Ad exchange requests bids from demand side platform
(CPM = cost per mille, or the cost to the advertiser to show this ad 1000 times)
Web Page
Ad
SSP
Ad Exchange
DSP 1
DSP 2
DSP 3
Advertiser 1
$0.9 CPM
Advertiser 2
$1.8 CPM
Advertiser 3
$0.2 CPM
Advertiser 4
$1.1 CPM
5. Ad exchange picks highest bid and sends winning ad's content to website
4. Demand side platforms respond with bids based on targeting

When you see an ad on a web page, behind the scenes an ad network has just automatically conducted an auction to decide which advertiser won the right to present their ad to you. Credit: Eric Zeng, CC BY-ND

Each day, you leave digital traces of what you did, where you went, who you communicated with, what you bought, what you're thinking of buying, and much more. This mass of data serves as a library of clues for personalized ads, which are sent to you by a sophisticated network—an automated marketplace of advertisers, publishers and ad brokers that operates at lightning speed.

The ad networks are designed to shield your identity, but companies and governments are able to combine that information with other data, particularly phone location, to identify you and track your movements and online activity.

More invasive yet is spyware—malicious software that a government agent, private investigator or criminal installs on someone's phone or computer without their knowledge or consent. Spyware lets the user see the contents of the target's device, including calls, texts, email and voicemail. Some forms of spyware can take control of a phone, including turning on its microphone and camera.

Now, according to an investigative report by the Israeli newspaper Haaretz, an Israeli technology company called Insanet has developed the means of delivering spyware via online ad networks, turning some targeted ads into Trojan horses. According to the report, there's no defense against the spyware, and the Israeli government has given Insanet approval to sell the technology.

Sneaking in unseen

Insanet's spyware, Sherlock, is not the first spyware that can be installed on a phone without the need to trick the phone's owner into clicking on a malicious link or downloading a malicious file. NSO's iPhone-hacking Pegasus, for instance, is one of the most controversial spyware tools to emerge in the past five years.

Pegasus relies on vulnerabilities in Apple's iOS, the iPhone operating system, to infiltrate a phone undetected. Apple issued a security update for the latest vulnerability on Sept. 7, 2023.

What sets Insanet's Sherlock apart from Pegasus is its exploitation of ad networks rather than vulnerabilities in phones. A Sherlock user creates an ad campaign that narrowly focuses on the target's demographic and location, and places a spyware-laden ad with an ad exchange. Once the ad is served to a web page that the target views, the spyware is secretly installed on the target's phone or computer.

Although it's too early to determine the full extent of Sherlock's capabilities and limitations, the Haaretz report found that it can infect Windows-based computers and Android phones as well as iPhones.

Spyware vs. malware

Ad networks have been used to deliver malicious software for years, a practice dubbed malvertising. In most cases, the malware is aimed at computers rather than phones, is indiscriminate, and is designed to lock a user's data as part of a ransomware attack or steal passwords to access online accounts or organizational networks. The ad networks constantly scan for malvertising and rapidly block it when detected.

Spyware, on the other hand, tends to be aimed at phones, is targeted at specific people or narrow categories of people, and is designed to clandestinely obtain sensitive information and monitor someone's activities. Once spyware infiltrates your system, it can record keystrokes, take screenshots and use various tracking mechanisms before transmitting your stolen data to the spyware's creator.

While its actual capabilities are still under investigation, the new Sherlock spyware is at least capable of infiltration, monitoring, data capture and data transmission, according to the Haaretz report.

Who's using spyware

From 2011 to 2023, at least 74 governments engaged in contracts with commercial companies to acquire spyware or digital forensics technology. National governments might deploy spyware for surveillance and gathering intelligence as well as combating crime and terrorism. Law enforcement agencies might similarly use spyware as part of investigative efforts, especially in cases involving cybercrime, organized crime or national security threats.

Companies might use spyware to monitor employees' computer activities , ostensibly to protect intellectual property, prevent data breaches or ensure compliance with company policies. Private investigators might use spyware to gather information and evidence for clients on legal or personal matters. Hackers and organized crime figures might use spyware to steal information to use in fraud or extortion schemes.

On top of the revelation that Israeli cybersecurity firms have developed a defense-proof technology that appropriates online advertising for civilian surveillance, a key concern is that Insanet's advanced spyware was legally authorized by the Israeli government for sale to a broader audience. This potentially puts virtually everyone at risk.

The silver lining is that Sherlock appears to be expensive to use. According to an internal company document cited in the Haaretz report, a single Sherlock infection costs a client of a company using the technology a hefty US$6.4 million.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

TechXplore

Citation: Spyware can infect your phone or computer via the ads you see online—report (2023, September 22) retrieved 6 May 2024 from https://techxplore.com/news/2023-09-spyware-infect-ads-onlinereport.html