Malvertising Surges to Distribute Malware

intel471.com/blog/malvertising-surges-to-distribute-malware

Many intrusions and compromises start with the infection of an endpoint with malicious software (malware). Malware distribution is often centered around tricking someone into opening an executable file that purports to be benign, such as a common software utility, but is actually malicious. One of the most common methods for distributing malware is through spam, but there are other ways. One long-used technique to land malware on systems saw a resurgence in December 2022.

“Malvertising” is a portmanteau of malware and advertising. It involves buying search engine advertisements and placing links in those ads that lead to malicious sites. The technique has been used by threat actors nearly as long as search-related, pay-per-click (PPC) ads have been around, but the recent surge was intense and unexpected. Here, Intel 471 explores how malvertising works, some defenses to employ against it and examples of how it was recently leveraged to distribute malware.

How PPC Works

Google’s PPC Ads platform is the primary medium actors use to distribute malware. Intel 471 analysts walked through the process of setting up a Google Ads campaign. The exercise revealed a great deal about how these actors conduct campaigns and some theories about how they obtain top search results for their advertisements.

Google’s PPC Ads management panel has a fairly intuitive design that allows users to view their advertisement campaign statistics at a glance. Users can view their current advertisements, keywords, recommendations, statistics and total cost for each offer. Users must supply a URL to create an advertisement, display paths for the URL, provide a description with the offer and craft some headlines for the advertisement. The descriptions, headlines and site are factored into the equation that Google uses to calculate the advertisement ranking.

Once an advertisement is created, users can set the maximum amount of money to spend on PPC for an ad. Advertisement space is sold using a blind auction mechanism where advertisers can outbid competitors but cannot see what others bid for advertisement space. Google’s old advertisement ranking algorithm previously considered how much advertisers bid to award advertisement placement rankings, however, the new system calculates a mix of advertisement bid price, description, headline and site checking.

Once users create an advertisement and set a bid price, they can begin using the multiple tools available on the Google Ads platform. Device targeting allows advertisers to set how much they want to bid on advertisements that will be shown only on certain types of devices, such as tablets or mobile phones.

Customers can use additional targeting available in the “Audience” tab of the Google Ads panel. Users can monitor the demographics for people who click on the advertisements, create targeted advertisements or exclude certain demographics and target specific types of people, such as those working in financial services or hospitality. The platform also allows advertisers to target customers based on geolocation in addition to audience tracking, or a variety of factors that include cities, states and postcodes.

Ppctargeting 2 A screenshot of the advertiser targeting options for the Google PPC Ads platform Jan. 26, 2023.

BokBot

BokBot, also known as IcedID, is a banking trojan that also doubles as a downloader for additional malware. The actors behind the development of BokBot historically had a relationship with the Conti ransomware group and Trickbot, another type of banking malware and botnet used to distribute ransomware. During the past year, initial access brokers (IABs) increasingly used BokBot as gateway malware for attacks in place of the now-defunct BazarLoader or Trickbot families. In December 2022 and January 2023, BokBot operators began experimenting with the Google PPC Ads platform for distribution.

The traffic distribution system (TDS) of these BokBot campaigns uses victim and bot filtering on the landing page where the Google Search Ads engine points. This filtering ensures that a connecting client is not coming from a virtual private network (VPN) IP address, makes user agent checks and follows hypertext transfer protocol (HTTP) "GET" header criteria. If a connection does not meet the criteria, the user is not redirected to the BokBot malicious landing page and instead stays on the advertisement site, which may or may not be related to the targeted app or brand. This site typically is unrelated to the campaign. Connections that meet the targeted criteria are redirected to the BokBot malicious landing page and will never see the advertisement site.

A recent BokBot campaign masqueraded as an advertisement for Docker, an operating system virtualization platform. The malicious advertisements contain typosquatted domains and appear higher than the legitimate offer for Docker. Once the user clicks on the ad link, BokBot's first typosquatting domain performs some basic bot filtering to determine whether the viewer of the advertisement is a legitimate victim to target and not a researcher. If the check fails based on user agent, user agent client hints or geolocation, the Docker campaign landing page will direct the viewer to a fake tutorial on how to set up and use Docker.

Dockersearchresults A screenshot of a malicious Docker advertisement that appears before both the legitimate Docker search results and advertisement Jan. 26, 2023.

BatLoader and EugenLoader/FakeBat

Malware loaders, also called "droppers," are the initial infections on systems which are then used by threat actors to download other malicious code. BatLoader, identified in February 2022, is a type of loader that leverages Microsoft software installers (.msi) and PowerShell.

Intel 471 recently uncovered that two different threat actors are distributing BatLoader through different command and control (C2) infrastructures. The campaign identified as BatLoader by Mandiant in 2022 involved the execution of .BAT files by the .MSI during install. A second campaign, however, does not involve the execution of .BAT files. Instead, that malware has an inline PowerShell script that is executed in place of the .BAT file. Due to these differences, Intel 471 analysts have decided to rename the second campaign to EugenLoader. It is also known as FakeBat.

As public reporting and our own reporting blended EugenLoader and BatLoader, it makes it hard to identify when EugenLoader first popped up. But it was likely running as of November or December 2022. During our investigation into EugenLoader, we found a domain that appeared to be used as the download destination for new campaigns. The root of the domain was mistakenly left open and revealed .MSI files for EugenLoader campaigns. As seen below, the EugenLoader malware had been renamed to impersonate known software such as FileZilla, uTorrent and WinRAR, among others.

Openindex The root directory of a domain for a suspected EugenLoader campaign was left open.

During distribution campaigns, EugenLoader stands up domains that purport to offer legitimate popular software but instead substitute malware for what is promised.

One of the most consistently active malvertising campaigns for EugenLoader masquerades as WinRAR, which is a popular software utility for compressing and extracting files. While other campaigns seemed to get their advertisement to the top of the search results intermittently, the WinRAR campaign has no such limiters. This enables the actors to trick victims into installing EugenLoader continually.

EugenLoader was also distributed via a malvertising campaign that spoofed 7-Zip, which is another popular file archiving software. Using well-crafted Google search advertisements, this campaign is able to place its download links before the official 7-Zip download page as observed in the image below.

7zipsearchresults 2 Two PPC ads appear offering 7-Zip but with domains that are not related to the official project. This screenshot was taken during a Germany-based browsing session Jan. 19, 2023.

Analysis

Until recently, malvertising was not a preferred initial access vector and seldomly was used compared to traditional vectors such as email spam. However, the operators behind EugenLoader were able to purchase advertisements that consistently appeared in the first search result position on Google. It should be assumed it is a dangerously successful technique that has the potential to challenge malware spam (malspam) as the go-to vector for criminals.

There are advantages and disadvantages for malware distributors to place malicious advertisements. First, an advantage: Bad actors capture an audience that is actively seeking out a tool to download. Appearing as the first search result means there’s a high probability someone may click without closely looking at the domain. The subsequent landing page then looks identical to the legitimate one, and people are likely to download and install the tool.

This has advantages over spam, which may be caught and quarantined by security tools or sent to the spam folder, never meeting the eyes of the potential victim. If it does reach the victim, the attacker must trick the person into taking action, such as opening an invoice, clicking on a link or running an executable. But malvertising catches people who want to download something and run it immediately.

Malvertising doesn’t come cheap, however. PPC ads could cost as much as US $2 to US $3 per click. Because bad actors are bidding for ad space, the actions also raise the costs for legitimate advertisers. It is possible malvertisers are paying for the ads with stolen credit card information. How bad actors are paying for the ads would be another research avenue to pursue, which could shed light on groups behind the campaigns.

In some cases, the success of campaigns could be gauged. Some of the malicious ads directed victims to sites hosted on Bitbucket, which may show the number of downloads. One campaign showed upward of 3,000 downloads. At US $2 a click, those who placed the campaign may have paid as much as US $6,000, which shows the attackers have financial means. Other types of malware seen in the campaigns included information stealers such as RedLine. The malware often thwarted VirusTotal submission. The file sizes were up to 700 MB, which is very large compared to the typical size of a dropper or loader. VirusTotal has a file size limit of 32 MB (files up to 200 MB may be submitted), which meant that malicious files distributed by the campaigns weren’t necessarily turning up later for analysis.

The malvertising surge, which mostly affected Google, appeared to peak in mid-January 2023 and has fallen since. The security community has been in touch with Google regarding its findings. Several researchers contributed to a spreadsheet that tracked malvertising campaigns and the brands that were impersonated. Between Jan. 19, 2023, and Feb. 22, 2023, the spreadsheet contained examples of 584 malvertising campaigns. Also, researchers created tools such as this one by Randy McEoin that can perform searches for malvertising and this one by Michael McDonnell that also takes screenshots of the campaigns. Hopefully, awareness has increased and defenses have been raised to minimize future malvertising campaigns.

Defensive recommendations

Intel 471 recommends customers consider deploying advertisement-blocking browser extensions such as the “AdBlock,” “Adblock Plus” or “uBlock Origin” supported browser extensions. These mitigate the appearance of Google PPC Ads traffic and prevent users from being duped into attempting to install malware masquerading as a legitimate application. Additional recommendations are to monitor for unauthorized MSIs and the installation and running of unsigned executables.

Special thanks to Jérôme Segura, senior director of threat intelligence at Malwarebytes, for help with this post.