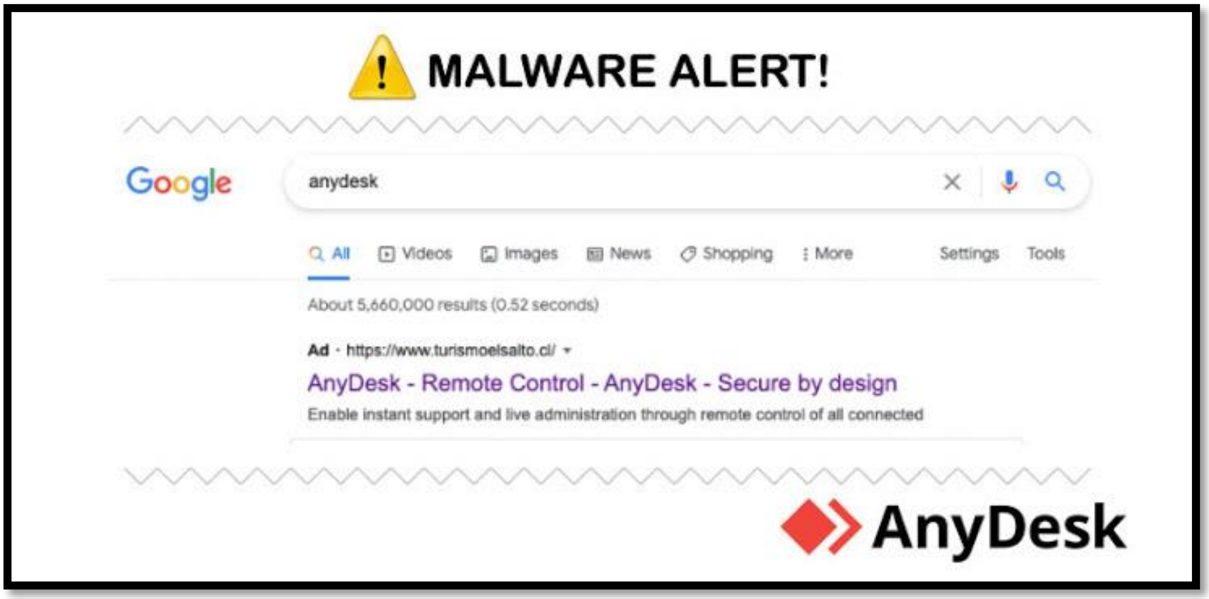
Malvertising Campaign On Google Distributed Trojanized AnyDesk Installer



About 5,660,000 results (0.52 seconds)

Ad · https://www.turismoelsalto.cl/

AnyDesk - Remote Control - AnyDesk - Secure by design

Enable instant support and live administration through remote control of all connected

Cybersecurity researchers on Wednesday publicized the disruption of a "clever" malvertising network targeting AnyDesk that delivered a weaponized installer of the remote desktop software via rogue Google ads that appeared in the search engine results pages.

The campaign, which is believed to have begun as early as April 21, 2021, involves a malicious file that masquerades as a setup executable for AnyDesk (AnyDeskSetup.exe), which, upon execution, downloads a PowerShell implant to amass and exfiltrate system information.

"The script had some obfuscation and multiple functions that resembled an implant as well as a hardcoded domain zoomstatistic.com to 'POST' reconnaissance information such as user name, hostname, operating system, IP address and the current process name," researchers from Crowdstrike said in an analysis.

AnyDesk's remote desktop access solution has been downloaded by more than 300 million users worldwide, according to the company's website. Although the cybersecurity firm did not attribute the cyber activity to a specific threat actor or nexus, it suspected it to be a "widespread campaign affecting a wide range of customers" given the large user base.

The fraudulent ad result, when clicked, redirects users to a social engineering page that's a clone of the legitimate AnyDesk website, in addition to providing the individual with a link to the trojanized installer.

CrowdStrike estimates that 40% of clicks on the malicious ad turned into installations of the AnyDesk binary, and 20% of those installations included follow-on hands-on-keyboard activity. "While it is unknown what percentage of Google searches for AnyDesk resulted in clicks on the ad, a 40% Trojan installation rate from an ad click shows that this is an extremely successful method of gaining remote access across a wide range of potential targets," the researchers said.

The company also said it notified Google of its findings, which is said to have taken immediate action to pull the ad in question.

"This malicious use of Google Ads is an effective and clever way to get mass deployment of shells, as it provides the threat actor with the ability to freely pick and choose their target(s) of interest," the researchers concluded.

"Because of the nature of the Google advertising platform, it can provide a really good estimate of how many people will click on the ad. From that, the threat actor can adequately plan and budget based on this information. In addition to targeting tools like AnyDesk or other administrative tools, the threat actor can target privileged/administrative users in a unique way."

Recommendations

- Use and update your antivirus software

Using a high-quality antivirus program is one of the first steps you should take when working on your cybersecurity. Keeping it up to date is the second one – especially when it comes to malvertising prevention.

When trying to prevent malvertising, make sure not to get tricked by fake security apps. While they claim to protect you, they may be spying on you instead – only use trusted providers for your cybersecurity.

- Consider using ad blockers

Even though relying on ad blockers alone is not sufficient, it’s a great starting point. These online tools block pop-ups and banner ads, hence you are less likely to suffer from malicious ads.

What you have to keep in mind, though, is that fraudsters have already come up with workarounds against ad blockers. Hence, using them with other tools (such as antivirus programs) is the only way to go. As an alternative, you can opt for ad filters, such as uBlock Origin.

- Update your browser and uninstall its plugins

Keeping your browser up to date is vital as it’s vulnerable to drive-by download attacks. The sooner you take care of all those necessary updates, the better.

References:

https://thehackernews.com/2021/05/malvertising-campaign-on-google.html
https://cybernews.com/security/what-is-malvertising/
https://us.norton.com/internetsecurity-malware-malvertising.html
https://www.avg.com/en/signal/what-is-malvertising