EINPRESSWIRE

New Malvertising Campaign Distributes Sophisticated Windows Backdoor via Google Ads

DUBAI, DUBAI, UNITED ARAB EMIRATES, April 23, 2024 /EINPresswire.com/ -- ANY.RUN warns of a new scam campaign that uses Google Ads to distribute Windows malware called MadMxShell. The malware uses DNS MX queries to communicate with its Command-and-Control server, hence the name.

This is the first time a campaign using Google Ads is used to spread a sophisticated Windows backdoor. The malware can collect system data, run commands via Cmd.exe and read, write, and delete files on the infected host.

According to the findings, the attackers registered over 45 domains between November 2023 and March 2024, impersonating legitimate IP scanning software such as Advanced IP Scanner, Angry IP Scanner, PRTG IP Scanner, and ManageEngine Advanced IP Scanner. When users search for these tools and click on the malicious Google Ads, they are tricked into downloading a malicious ZIP archive containing the backdoor.

The infection chain involves a multi-step process: DLL side-loading and process hollowing are used to inject malicious code into a legitimate process and evade detection. Analysis in the ANY.RUN cloud interactive sandbox shows that MadMxShell uses additional evasion techniques, such as delays introduced by executing ping commands, to avoid detection in automated sandboxes that have a limited time window for analysis.

To protect against malvertising, users are advised to be careful when clicking on ads - it is safer to visit organic search results. In addition, before running any program downloaded from the

Internet, it is advisable to run a file in a sandbox, such as ANY.RUN, which records and highlights any potential malicious activity and displays it clearly in reports. Organizations can use sandboxing to collect malware IOCs and configure their security systems accordingly.

Learn more in ANY.RUN blog.

Vlada Belousova
ANYRUN FZCO
+1 202-788-9264
email us here
Visit us on social media:
Twitter
YouTube