Hive Pro

THREAT ADVISORY

AnyDesk Installer Targeted by Malvertising Campaign

TA202116

Threat Level Green

Publish Date – May 30, 2021

A malvertising campaign, which was active since April 21, was established by hackers for a popular remote desktop application, AnyDesk. A fake app ad was pushed via Google ads when searching for "AnyDesk". The App contained trojan malware that could control the victim's computer. That ad redirected users to a URL: https://domohop.com/anydesk-download/ which then downloads the trojan file with link: https://anydesk.s3-us-west-1.amazonaws.com/AnydeskSetup.exe

40% of these ads lead to downloading and installing this trojan file. And 20% of these installations lead to getting a follow-on hands-on-keyboard activity. Hackers have reportedly paid Google $1.75 per click.

Indicators of Compromise

Type	Value
IP Address	176.111.174.126 176.111.174.125
Domains	Domohop.com Anydesk.s3-us-west-1.amazonaws.com zoomstatistic.com anydeskstat.com Turismoelsalto.cl Rockministry.org curaduria3.com
User Agents	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100111 Firefox/78.0
Hashes	357e165be7a54e49f04cccc6d79678364394e33f10a6b3b73705823f549894b5 5fe992b5a823b6200a1babe28db109a3aae1639f0a8b5248403ee1266088eac4 0c1ec49bf46f000e8310ec04ff9f5a820cbb18524acf8e39482ae3ffca14fb59 780a02755873350ceef387fd9ea8c9614d847d5ba7ae3f89d32777b6ec7ee601

References

https://www.crowdstrike.com/blog/falcon-complete-disrupts-malvertising-campaign-targeting-anydesk/
https://cybersecuritynews-com.cdn.ampproject.org/c/s/cybersecuritynews.com/weaponized-anydesk-installer/?amp