Jan 30th, 2023

Current Event- 1

***Malicious Use of Google AdSense***

We all have seen advertisements popping up all over the internet. Especially when we search for something through the google search engine, in most cases, the top results are advertisements with URLs prefixed with an ad. Malicious actors clone a genuine website, then buy a lot of advertisements to place it on the top of google search results to gain traffic. When the victims click on the ad, they are taken to the cloned website, except the application download link contains a malicious application instead of a genuine one. The current trend is crypto-jacking the victim's hardware resources. For our case, the applications are intense graphic applications like OBS and Blender.

It is pretty accessible to anyone to disguise a malicious URL with a genuine-looking URL using an IDN homograph attack. There are many tools on the internet to make this possible. Once the victim installs the malicious application, their sensitive information, from credit card details to cryptographic wallets, is sent to the attacker. Here the infected applications act as a trojan. We use many open-source applications like WinRAR, 7-Zip, VLC Media Player, Notepad++ in our day-to-day life. These applications are the most widely observed targets of malicious actors. It is no one's fault, not Google’s or the application developer's. The users are at fault for falling into the attacker's trap. Even with a robust system in place, humans are the weak point. Here Confidentiality of the victims has been compromised.

Google's AdSense is not going anywhere; it is one of Google's cash cows. Google can make stringent policies on who can use its AdSense and verify whether it is a legitimate customer. Educating the general public on how to be safe on the internet helps a little bit in this case. We cannot address every situation. However, we can inform the public as soon as we find a significant mass malware distribution like this. CIA issued a public safety announcement to install Adblockers. Google can also review its current AdSense contracts to find these malicious actors by relating a website's content to its URL.

Ionut Ilascu (2023, January 17). *Hackers push malware via Google search ads for VLC, 7-Zip, CCleaner*

<https://www.bleepingcomputer.com/news/security/hackers-push-malware-via-google-search-ads-for-vlc-7-zip-ccleaner/>

Seytonic (2023, January 25). *Hacked From a Google Search*

<https://www.youtube.com/watch?v=xcqiERpYlmM>