Dirty SEO campaign brings a series of malicious software to the top of search

Cybercriminals are using dirty SEO methods to bring malicious software to the top of search.

A large-scale dirty SEO campaign is being conducted by cybercriminals. By different methods, they bring fake versions containing malicious code of popular software to the top of search. If the user clicks, downloads and installs it, it will immediately be infected with the BATLOADER malware.

In a newly published report, Mandiant researchers detailed a dirty SEO campaign. "Hackers used SEO keywords like "install free productivity apps" or "install free software developer tools" as keywords to lure victims to visit and download the installers. contains malicious code".

Attacks by means of SEO poisoning, hackers increase the ranking of malicious download pages to make them show up at the top of search results. When users search for apps like TeamViewer, Visual Studio and Zoom they will see fake pages at the top. If the victim accesses and downloads that fake software, the victim will be infected with malicious code.

While packaging the installer, the hacker adds the BATLOADER malware. Therefore, when installed, malware will also be installed on the victim's machine. BATLOADER will download other executables to probe the target. Next, other malicious code is also downloaded to be installed to carry out a chain of infection.

Other additional malware installed include Atera Agent, Cobalt Strike Beacon and Ursnift. They will perform behaviors such as remote monitoring, privilege escalation, and credential collection.

To avoid becoming a victim, users should not download cracked or free software from unauthenticated sites. In addition, you should carefully check the address of the site where you intend to download the software to avoid accessing the fake site. Finally, before installing, use anti-virus software to scan the installation file.