Pirated games aren't free - they will cost you time, money and security

By June 2021, Crackonosh, a complex cryptojacking malware, earned threat actors a hefty profit of $2m. Once in a system, the malware destroyed any antivirus programmes installed and then set about mining cryptocurrency. This malware is one of many that's found its way into systems, riding on the back of cracked games that are offered for free on torrent or download services. Anna Collard, SVP of content strategy and evangelist at KnowBe4 Africa, points out, if you want the fun for free, you may pay a heavy price when getting infected.

Anna Collard

“Cracked copies of popular software or games often come with built-in malware that searches for, and disables, many of the most well-known antivirus programmes,” she explains. “For example, Microsoft Office and Adobe Photoshop are incredibly popular which means cracked versions are always going to be in demand.”

Bitdefender found that certain versions of both Microsoft Office and Adobe Photoshop were being distributed with malware that was capable of stealing browser session cookies, or the entire user profile history if they use Firefox, hijacking Monera cryptocurrency wallets, and exfiltrating other data via BitTorrent.

“This malware opens a back door, turns off the firewall, and then leaves everything wide open to attack,” says Collard. “This doesn’t only put the system at risk of the virus that’s currently wreaking havoc, but at risk of being infected by other malware because the protection is down.”

Cracked games can also introduce adware, trojans and spyware onto target machines. Choosing to download a free crack instead of paying for the full product is a high-risk strategy that isn't exclusively limited to PC gamers. Mobile devices and applications are just as dangerous, although often not for the same reasons. Where downloading cracked games is the PC equivalent of diving into a pool filled with viruses, mobile games are a different story.

"Today, clickjacking and malicious apps are two of the most common forms of mobile fraud," says Collard. "Using clickjacking, fraudsters can intercept a legitimate click and direct the user to a website that steals sensitive information. Malicious apps have been injected with malware during a disguised app update or when downloaded from somewhere other than the official app store"

According to the Evina State of Mobile Fraud in South Africa report, from January to June 2021, 29.5% of mobile transactions were identified as suspicious. What's worse, 76% of them were related to clickjacking and 5.6% to malicious apps. This makes it increasingly important for people to understand exactly what the risks are, and how to practice good safety hygiene across all devices and technology touchpoints. The reality is that the hackers are making far too much profit, far too easily, to stop. So, the protection of your assets and the security of your systems lies with you.

"Downloading cracked games is always going to be a risk," concludes Collard. "Even sites that claim to be virus-free can be owned by hackers – there are absolutely no guarantees. So, to stay safe, only use legitimate software and keep it updated, use antivirus protection, and don't click on any suspicious links."