Issued 5/29/17

'Judy' Could Be the Largest Malware Campaign ever Found on Google Play Store

Security experts have uncovered a massive malware campaign spreading through Google Play, the marketplace used to download applications to phones and tablets. Dubbed "Judy", the malicious software is a form of "auto-clicking adware" downloaded millions of times. Researchers from Check Point, a cybersecurity firm, claimed this week (25 May) it could be "possibly the largest" malware campaign found on Google Play.

The suspicious code was observed in more than 40 applications, most allegedly developed by a Korean company called Kiniwini. Once downloaded by a victim, the malware stealthily connects to a command and control (C&C) server which then sends it a slew of URLs defined by the developers. It opens the website domains in a hidden webpage and proceeds to automatically click on advertising banners to make money via Google Ads. One application singled out by Check Point, called Chef Judy: Picnic Lunch Maker, was updated on 10 April 2017. The total amount of downloads in total from all affected apps in the campaign reached between 8.5 and 36.5 million, the experts claimed.

The "Judy" campaign also displays a large amount of advertisements on selected apps which leaves the user with no option other than clicking. It remains unknown how much money the developers have made from the

malware attacks, but Check Point said it would be a "large revenue." The experts said there was two distinct campaigns potentially using shared malicious code. All updated within the last few months, other apps titles included Fashion Judy: Snow Queen Style, Fashion Judy: Vampire style, Chef Judy: Character Lunch and Fashion Judy: Frozen Princess. Each boasted downloads ranging from 10,000 to a million, the researchers found. "Some of the apps we discovered resided on Google Play for several years, but all were recentlyupdated. It is unclear how long the malicious code existed inside the apps, hence the actual spread of the malware remains unknown," the team said in a blog post. It continued: "We also found several apps containing the malware, which were developed by other developers on Google Play. The connection between the two campaigns remains unclear, and it is possible that one borrowed code from the other, knowingly or unknowingly. "After Check

Point notified Google about this threat, the apps were swiftly removed." Kiniwini, registered on Google Play as EniStudio, develops smartphone apps for both Android and Apple iOS. On its website (translated via Google) the company published a statement informing users the app was removed but claimed new software will be released within two months. It said: "Our game apps have been blocked on Google Play and the service has been stopped. "Unfortunately, existing games can no longer be downloaded from Google Play. Users who have already installed the game and have not deleted it are still able to use it. Apple App Store is available as usual. Jean-Chefs Judy and Animal Judy Season 2 will be released in July." There has been a spike in reported Play Store malware incidents in recent weeks, with other strains known as "BankBot" and "FalseGuide" slipping through the marketplace's censors. This week, on 24 May, it was revealed developers had been peddling fake "protectors" for ransomware. "Users cannot rely on the official app stores for their safety," Check Point warned. Google did not immediately respond to a request for comment.