Security and Proprietary Software

By Roy Schestowitz
Created 25/04/2021 - 5:02am

- New cryptomining malware builds an army of Windows, Linux bots [3] [Ed: reminder never to put SSH keys on Windows, machines and other back-doored OSes [4]]

  After hacking [sic] into a server and killing competing cryptocurrency miners, the malware will also spread over the network in brute force attacks using SSH private keys collected from various locations on infected servers

- Critical RCE Bug Found in Homebrew Package Manager for macOS and Linux [5] [Ed: This is a Microsoft (GitHub, proprietary software) issue, not "macOS and Linux". Microsoft loves blaming the victims for its own failures [6].]

  A recently identified security vulnerability in the official Homebrew Cask repository could have been exploited by an attacker to execute arbitrary code on users' machines that have Homebrew installed.

  [...] The researcher also submitted a proof-of-concept (PoC) pull request demonstrating the vulnerability, following which it was reverted. In light of the findings, Homebrew has also removed the "automerge" GitHub Action as well as disabled and removed the "review-cask-pr" GitHub Action from all vulnerable repositories.
HashiCorp is the latest victim of Codecov supply-chain attack [7] [Ed: Microsoft’s close partners (in crime) cannot do security]

The company states that as a result of this, the GPG key used by HashiCorp to sign and verify software releases was exposed.

Codecov provides software testing and code coverage services to over 29,000 customers.

On April 1st, Codecov had learned that due to a flaw in their Docker image, threat actors had obtained credentials to the Bash Uploader scripts used by their customers.

How Not To Run A Vulnerability Disclosure Program [8]

AmEx has now twice refused my free donation of security information: first when they handed me off to some third-party service bot which demanded I agree totally to their terms or fuck directly off, and second when the third-party service they picked turned out to be run by idiots that have decided that graceful degradation in the face of feature incompatibility, one of the core foundational tenets of the world wide web since its invention, despite a nice two-decade run simply isn?t important anymore in 2021, and that serving blank pages to? you know, security professionals with javascript disabled (pretty much browser security tip #1), is totally fine.

How racism found my son on Fortnite [9]

Fortnite is a wildly popular free third-person shooter video game. For [Internet] babies like Waylon, Generation Alpha ? kids born after 2012 ? mastering the [Internet] and related technology like Fortnite is their rite of passage. These tech-savvy children navigate technology that makes them far more advanced than children of my era. Artificial Intelligence, facial recognition, and VR stand no chance with an Internet Baby. Once they get the hang of it, it's a wrap. What Fortnite offers to these highly advanced yet still impressionable children and teens is it allows them to bond with other children of different races and cultures while hooking them on the same poisonous pop culture we’re all exposed to, all via video game play.

In Fortnite, a player in survival mode gathers resources, weapons and tools to create bridges and forts as a means of survival. Sorta like The Simms times Final Fantasy on steroids, and the 100-player Battle Royale is similar to a last man standing match in pro wrestling. It has a colorful cartoon scheme that is constantly updated with celebrity skins, trending themes and music. It's addictive, and no wonder ? for [Internet] babies, Fortnite is like their Instagram newsfeed.

Convicted Post Office workers have names cleared [10]
The clearing of the names of 39 people follows the overturning of six other convictions in December. This means more people have been affected than in any other miscarriage of justice in the UK.

●


The composition of the board and the descriptions of the board members’ backgrounds suggest that it might not be entirely wrong to call the Bill and Melinda Gates Foundation (BMGF) and the IFLA Global Libraries Foundation merry bedfellows. It thus seems to be the case that the latter has been founded in order to be able to conveniently channel money and influence from the former to IFLA.

This impression was significantly strengthened when I studied the annual accounts of IFLA’s finances over the past four years. These are found at Ifla.org. To get an overview, I compiled the following table: […]

[...]

Many of us must have noticed that Bill Gates and Mrs. Melinda, through their BMGF and its huge capital, exercise a significant influence in the present world. But who could have guessed that they have taken such a firm grip on the entire global library development?

Software Security

Source URL: http://www.tuxmachines.org/node/150415

Links: