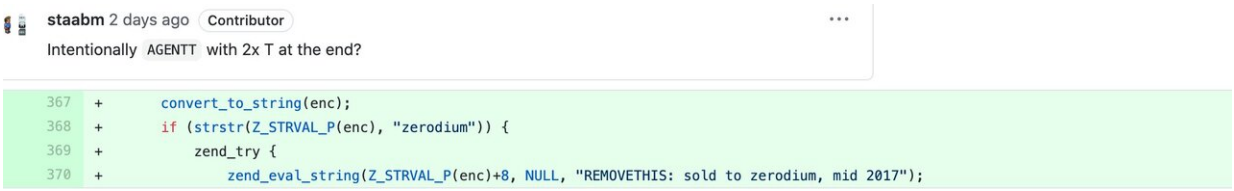
Security researchers announce PHP backdoor

March 30 2021, by Sarah Katz



Malicious Zerodium Commit. Credit: GitHub

On Saturday, 28 March 2021, security researchers Nikita Popov and Rasmus Lerdorf announced the discovery of two malicious backdoors installed on the php-src repository. The researchers suspect that this mishap had something to do with a compromised git.php.net server rather than a compromised individual git account.

In the meantime, while the research team works to get to the bottom of the issue, they have deemed continued use of their own git infrastructure as an unnecessary risk and will therefore cease use of the git.php.net server. Now, the related repositories on GitHub will go from being mirrors to actual canonical repos. As a result, any changes should be pushed to GitHub directly rather than through git.php.net.

To harden security status, repository users will now only have write access via the PHP organization on GitHub instead of the repo's native

karma system. As organization membership requires the use of two-factor authentication, users who wish to join the repo should contact Nikita directly with their GitHub account and php.net account names as well as the permissions to which they require access.

Finally, this change has made it impossible to merge pull requests directly from the GitHub web interface.

On the technical side, so far it appears as though the attackers gained code-execution abilities through knowledge of the secret password "zerodium". The hackers used an account disguised as belonging to researcher Lerdorf as a means to carry out this malicious activity. The subsequent malicious change was made via Popov's account name.

Zerodium is actually the name of a company that purchases exploits from researchers and sells them to government agencies for the purpose of cybersecurity investigations. However, while both malicious commits used to initiate these code changes reference Zerodium, the CEO Chaouki Bekrar insists the organization had no involvement. In fact, Bekrar even suggested that researchers themselves wanted to destroy evidence of the commit after failure to sell the backdoor.

This incident harkens back to a similar event in early 2019 which involved the popular PHP Extension and Application Repository temporarily shutting down the majority of the platform after finding that hackers had replaced the main package manager with a malicious package. Like this most recent incident, users of the impacted repository who registered within the past six months could be infected.

As of yet, the estimated 80 percent of websites operating on PHP do not seem to have run this evil commit in their production environments.

More information: "Changes to Git Commit Workflow." PHP,

GitHub, 28 Mar. 2021, news-web.php.net/php.internals/113838