ADVISORY REPORT ON

PHP Git repository hack

CyberPeace Foundation

Advisory report on PHP Git repository hack

CyberPeace Foundation

Date : 26th April 2021
Problem ID & Name : PHP Git Repository Hack
Severity : Medium

Executive Summary

A suspicious threat actor compromised the popular server-side language PHP's git repository. It is believed that the attacker committed a couple of changes to its source code repository that had a backdoor and allowed a Remote Code Execution (RCE) the maintainers of the project revealed. PHP is a widely used server-side programming language and almost used by 80% of the websites. So far, the intentions of the attackers is unknown and upon investigating this in depth it came into light that the commits were made under the names of legitimate members.

```
Usage statistics of PHP for websites
This report shows the usage statistics of PHP as server-side programming language on the web.
See technologies overview for explanations on the methodologies used in the surveys.
Our reports are updated daily.
PHP is used by 79.2% of all the websites whose server-side programming language we know.
```

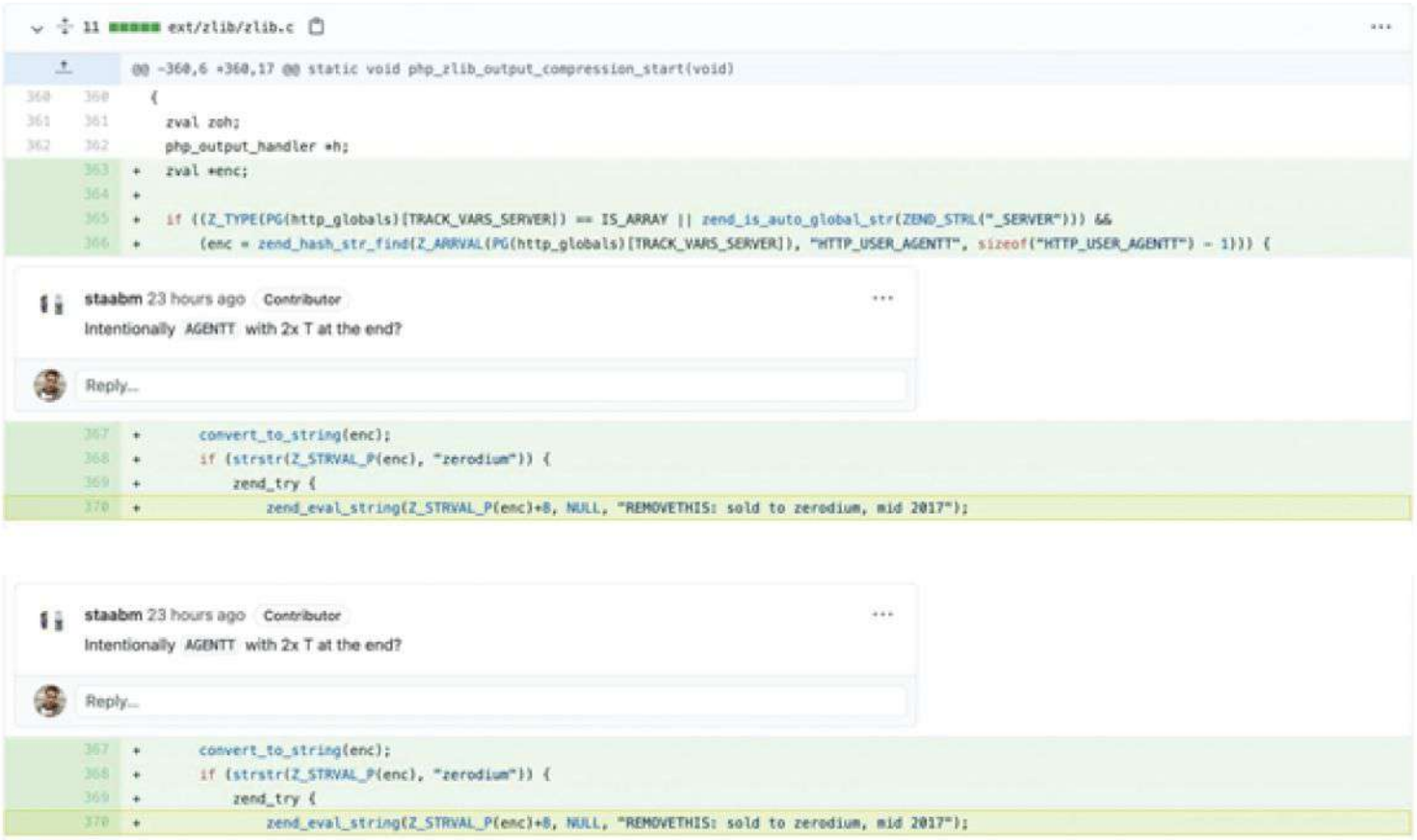
Digging deeper into the issue, it was found that the code created a backdoor that allowed attackers to take control over any website that used PHP remotely. In a statement released by one of the chief maintainers, the attackers have found a way to hack the server on which the repository was hosted. He further added PHP is investigating into the repositories for the matters of corruption beyond the couple of recently made commits. Since this attack did not cause the carnage as expected, we categorise it under medium severity.

```
Changes to Git commit workflow
From:
Nikita Popov Subject Changes to Git commit workflow php.doc php.internals
Date:
Groups:
Hi everyone,
Sun, 28 Mar 2021 22:52:24 +0000
Yesterday (2021-03-28) two malicious commits were pushed to the php-src repo [1] from the names of Rasmus Lerdorf and myself. We don't yet know how exactly
this happened, but everything points towards a compromise of the git.php.net server (rather than a compromise of an individual git account).
While investigation is still underway, we have decided that maintaining our own git infrastructure is an unnecessary security risk, and that we will
discontinue the git.php.net server. Instead, the repositories on GitHub, which were previously only mirrors, will become canonical. This means that changes
should be pushed directly to GitHub rather than to git.php.net.
While previously write access to repositories was handled through our home-grown karma system, you will now need to be part of the php organization on GitHub.
If you are not part of the organization yet, or don't have access to a repository you should have access to, contact me at nikic@php.net with your php.net and
GitHub account names, as well as the permissions you're currently missing. Membership in the organization requires 2FA to be enabled.
This change also means that it is now possible to merge pull requests directly from the GitHub web interface.
We're reviewing the repositories for any corruption beyond the two referenced commits. Please contact security@php.net if you notice anything.
Regards, Nikita
[1] : https://github.com/phrl/php-src/commit/c730aa26bd52829a49f2ad284b181b7e82a68d7d and https://github.com/phialphp-src/
commit/2b0f239b211c7544ebc7a4cd2c977a5b7aned8a
```

As per the mitigation and recommendation

As a mitigation step for the future, the maintainers have decided not to accept any commits on the main server. However, the changes can be made on GitHub. Both the commits are fix a typo of commits according to the maintainers.

The amendments to the code were first spotted by the contributors and one of them revealed that a particular line of code executes from a user HTTP header if the string begins with zerodium. It is one of the leading companies that buys zero-day exploits .



As you can see in the above screenshot where the backdoor is implemented and the threat actors can gain the access remotely/ In addition to this the chief maintainer of the repository said, they are going to implement MFA after the attack, making sure this is not repeated in the future.

References

1) https://portswigger.net/daily-swig/backdoor-planted-in-php-git-repository-after-server-hack

2) https://threatpost.com/php-infiltrated-backdoor-malware/165061/

3) https://www.welivesecurity.com/2021/03/30/backdoor-php-source-code-git-server-breach/

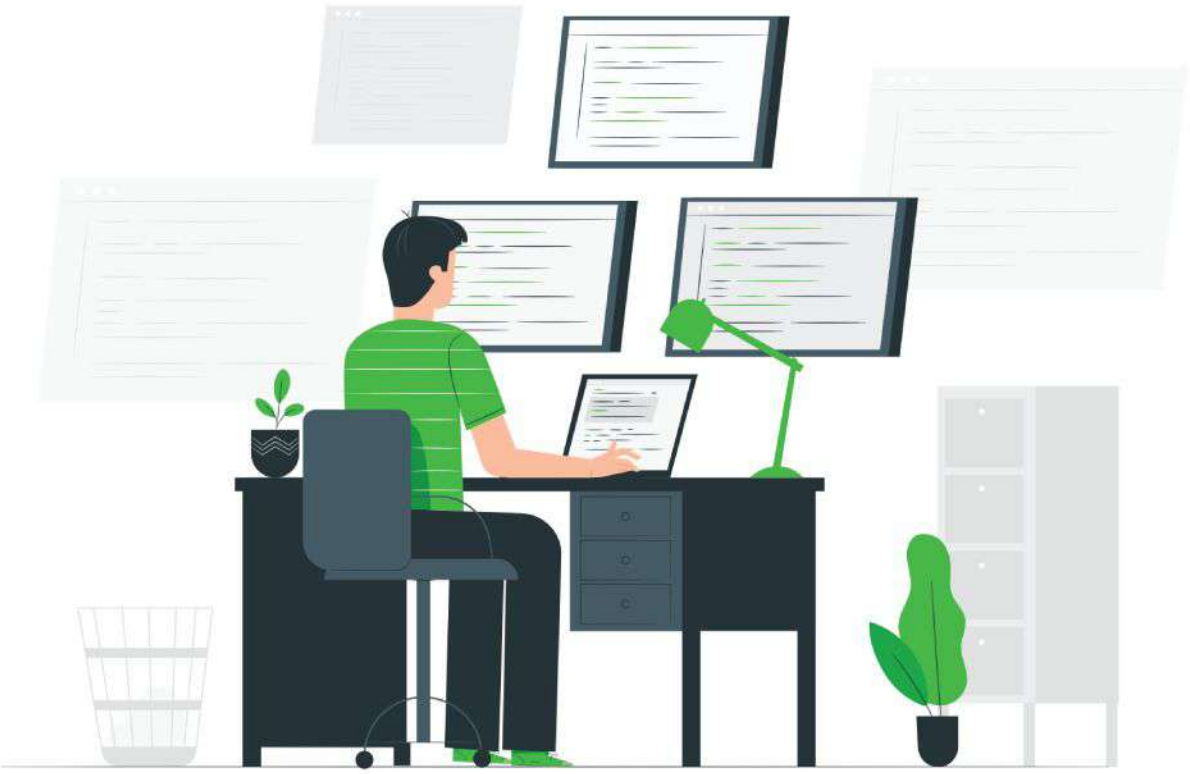
Revision Table :

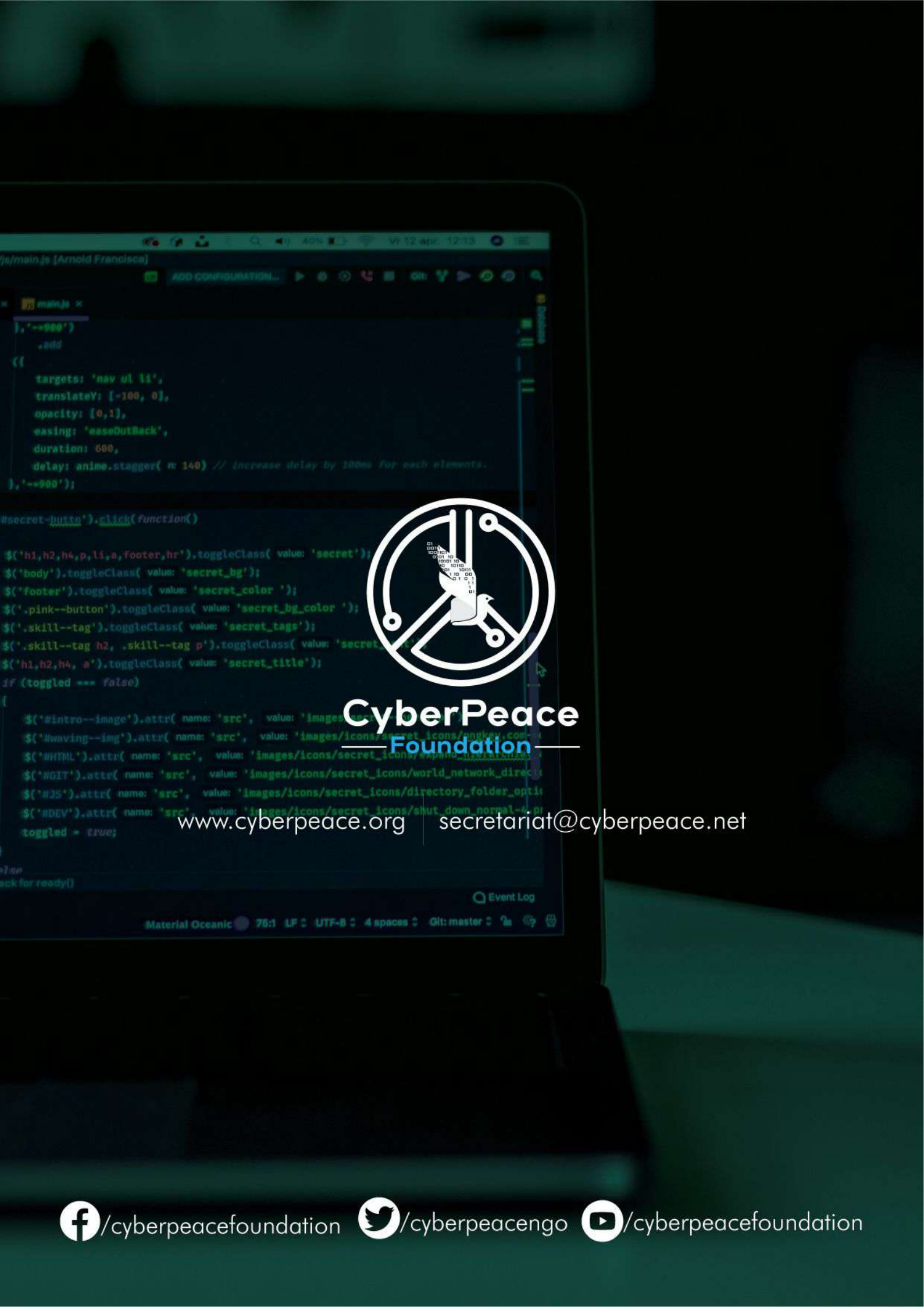
SI. NO.	DESCRIPTION	STATUS
1	Initial Public Release	Final

Issued by

Research wing; CyberPeace Foundation

Research Wing, Autobot Infosec Private Ltd.




CyberPeace
Foundation
www.cyberpeace.org
secretariat@cyberpeace.net
/cyberpeacefoundation
/cyberpeacengo
/cyberpeacefoundation