Hackers use recycled backdoor to keep a hold on hacked e-commerce server

reader comments

27 with 20 posters participating

Share this story

Who needs a better mousetrap when the old one is fine?

That was the approach of hackers who recently compromised a server running open source e-commerce platform Magento. To guard against the possibility of being locked out of the server should the rightful operators ever discover the breach, the attackers left behind a simple but effective script.

To the naked eye, the script was easy to miss amid countless other Magento files. Examining the code inside, however, revealed that it was a backdoor that was activated by sending the server a simple and innocuous-looking Web request. With that, an attacker who otherwise might have been booted out of the server could instantly become a server administrator with unfettered control of the system.

The script—with 92 lines including comments and empty lines—is effective and easy to overlook, said Krasimir Konov, a malware analyst at website-security firm Sucuri who recently spotted it. One thing the script is not is new. Konov said it is pretty much a mirror copy of code he first saw in 2012 and of samples subsequently documented in 2013 and 2014.

“My guess would be that somebody was too lazy to write their own script, so they just copied this from somewhere and used it in their attacks,” Konov told me on Tuesday. “These scripts are just as effective, with little modifications needed to work on newer versions of Magento.”

The effectiveness of the backdoor is its ease of use. The admin password and everything else the attacker needs is coded into the script. All that’s needed, in the event the hacker is ejected, is to send a Get request to the location of the script file. With that, the attacker has a new admin account that uses the username, password, and email address of their choice.

The script has a few other tricks for added stealth. The newly created admin account acquires all rights, meaning it likely becomes a new administrative role for the website. This may conceal the user if anyone checks the list of admins within the Magento CMS. Once the new admin account is created, the script deletes itself.

Here are images and brief descriptions of the script:

- Variables for creating the new user.
- Ensure Magento is installed by checking for the a//Mage.php file.
- Create a new user with the previously defined variables.
- Give the new user all permissions.
- Add the malicious user to the new role group.
- Delete the script.

Konov said he’s not sure how attackers managed to install the script on the server he recently disinfected. Because the Web server was running Magento 1.9.4.2, he suspects they exploited one of the many vulnerabilities found in that version (for instance, this one or this one). He said he can’t be sure, since he didn’t perform a forensic analysis.

However the backdoor got there, its continued use suggests it continues to work.

In a post published Tuesday, Konov wrote: “If the backdoor isn’t properly removed from the website’s environment, the file can remain and be used over and over to add new users with elevated privileges—especially if a website owner is unaware of the infection or thinks that simply removing the new user from Magento is enough to prevent unauthorized access.”

https://arstechnica.com/?p=1693361