Detects campaigns looking for large-scale Adminer database administration tools

Sucuri, a newly acquired network security company, GoDaddy discovered a large-scale search campaign to find websites using Adminer's database administration scenario.

Sucuri, a newly acquired network security company, GoDaddy discovered a large-scale search campaign to find websites using Adminer's database administration scenario.

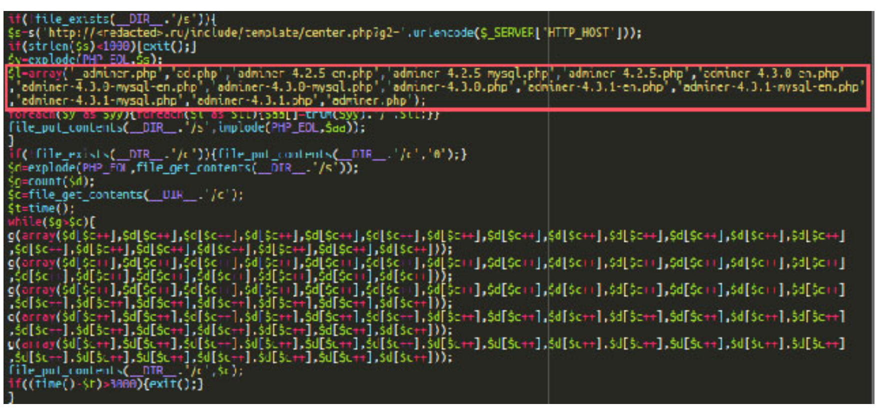
Adminer is a tool similar to phpMyAdmin but has a smaller size and less features, which is why it is so popular in the world of webmasters.

Adminer has been present for over a decade and because of its compactness, it is used on many servers and embedded into many popular CMS platforms such as WordPress, Drupal, Joomla, Magento .

Due to its intended use, anyone who has captured the Adminer account is also able to execute SQL query commands on the server. Hackers can easily use these commands to hijack the server and indirectly control all websites running on it.

Detect campaigns to scan Adminer search

Scuri, the company that is running one of the best Web Application Firewall (WAF) in the market, said that they found signs of scanning for the Adminer on the website they were investigating.



Discover Adminer search engine on website

Researcher Denis Sinegubko says he has found a valid file hiding system called at.php, which executes a query to a remote server for 10,000 domains ordered alphabetically. The scan tool then connects to these domains and

finds 14 files with the same names as Adminer's script or plugin.

Sinegubko said that once the detection page is running Adminer, it will save the page and the URL is working into a file with a simple name 'c'. After scanning, it will continue to work with other domains.

We can only estimate that the attacker either uses one of the Adminer vulnerabilities to gain access to the database management interface or to use the wrong test method to break into the instance. Adminer has a default or easy-to-guess password.

Adminer as well as phpMyAdmin, SQL Buddy and similar tools, does not have a protection system against the wrong type of attack. Webmasters who use a web-based GUI to manage databases need to consider switching to the CLI interface or installing WAF. If you can't use the free versions, you can use free tools like ModSecurity or NinjaFirewall.