Incident Report: Project 2

Date: 2025-03-16
Handler: Rilijin G Carrillo

Executive Summary

On February 3, 2021, the Cyber Security teams discovered that a WordPress blog used for research had been hacked. The site was altered to show advertisements for essay-writing services. After investigating, it was found that the attacker used a brute-force attack on the XML-RPC API to gain admin access. Once inside, they created a new admin account and changed the site's content. The attacker may have also leveraged outdated WordPress files, such as **TIMTHUMB**, which can be exploited to modify images and gain system access. To fix the issue, unauthorized accounts were deleted, backups were restored, and security measures were put in place. The estimated financial impact of this incident is **$7,000**.

Background

The affected system was a WordPress blog. It was mainly used to share research updates. The website had basic security but allowed XML-RPC functionality, which became the main target of the attack. Additionally, there were traces of activity involving the outdated **TIMTHUMB** file, which attackers often exploit to gain unauthorized access. The security team noticed unusual activity on February 3, 2021, at 09:32 AM EST, when IP 47.75.76.54 sent over 1,000 POST requests to xmlrpc.php in just ten minutes. This looked like a brute-force attack meant to guess passwords. Later, on February 6, 2021, at 11:40 PM EST, IP 157.75.167.23 was caught accessing the WordPress admin panel, likely using stolen credentials or a new unauthorized admin account.

Timeline

- **February 1, 2021**
    - **07:56 PM EST –** The legitimate admin account (admin) was created.
- **February 3, 2021**
    - **09:32 AM EST –** Unusual activity begins with multiple login attempts targeting xmlrpc.php.
    - **09:42 AM EST –** Attack stops after over 1,000+ POST requests.

10:00 AM EST – Security team is notified, and IP 47.75.76.54 is blocked (It's possible the attacker may have switched to a different IP address).

    - **10:00 AM EST –** XML-RPC functionality is disabled to stop further attacks.
    - **11:00 AM EST –** Log files are reviewed to check for other suspicious activity, including POST requests related to /wp-content/plugins/wordpress-gallery-plugin/bbb.php, which were determined to be regular traffic.
    - **01:00 PM EST –** IT administrators are informed, and security policies are reviewed.

- **February 4, 2021**
    - **02:23 PM EST –** A different malicious IP attempts to access timthumb.php multiple times before succeeding on the fifth attempt.
- **February 6, 2021**
    - **11:40 PM EST –** The unauthorized admin account (admin2) is created with full administrator privileges.
    - **11:40 PM EST –** IP 157.75.167.23 is found making multiple POST and GET requests to admin-ajax.php, which suggests further unauthorized access.
- **February 7, 2021**
    - **10:00 AM EST –** The unauthorized admin account (admin2) is removed.
    - **10:30 AM EST –** Spam content injected into the website is deleted.
    - **12:00 PM EST –** The site is restored using a clean backup.
- **February 8, 2021**
    - **09:00 AM EST –** Additional security improvements are made, including rate limiting, stronger authentication, improved alarm systems, and intrusion detection.
    - **04:00 PM EST –** Incident response officially concludes.

Findings

The attack started with a brute-force attempt against xmlrpc.php, where over 1,000 login attempts were sent in a short period. Since XML-RPC allows remote logins, this was an easy way for the attacker to constantly try different credentials. Also, there were attempts to exploit the outdated **TIMTHUMB** file, a vulnerability that allows attackers to manipulate images and potentially gain deeper system access.
After the attacker gained admin access, they modified the wp_posts table in the WordPress database to insert spam content advertising essay-writing services. Logs later showed that IP 157.75.167.23 interacted with admin-ajax.php, which suggests that the attacker continued making changes or attempting to install further modifications to the site.

Actions Taken

To stop the attack, the security team blocked the attacking IP address (47.75.76.54) and disabled XML-RPC to prevent further brute-force attempts. A detailed review of the server logs helped identify additional suspicious activity, leading to further investigations. IT administrators were notified, and new security measures were put in place. To prevent future brute-force attacks, rate limiting was added to detect and stop excessive login attempts. Improved alarm systems were also added to alert administrators about suspicious activity earlier. Security teams also monitored for any ongoing threats and flagged IP 157.75.167.23 for further investigation. Finally, the unauthorized admin account (admin2) was deleted, the injected spam content was removed, and the website was fully restored from a clean backup.

Financial Impact

Item	Cost
Investigation (15 hours x $100/hr)	$1,500
Incident Response Efforts	$2,500
Security Enhancements & Monitoring	$1,000
Business Downtime	$2,000
Total	**$7,000**

Lessons Learned

Successes

One of the biggest successes in this incident was how quickly the security team identified the brute-force attack. The logs showed the excessive requests to xmlrpc.php, which helped the team detect and respond before more damage was done. Blocking the attacking IP and disabling XML-RPC right away helped contain the attack early on. Another strength was the backup and recovery process. Once the unauthorized changes were found, the team restored the website from a clean backup, which minimized downtime. The IT department did a great job in coordinating with the security team to review policies and apply security patches to prevent further issues.
Action Item Owner: IT Security Team

Opportunities for Improvement

Issue: The attack succeeded because there were no strong authentication requirements in place, and XML-RPC was left enabled by default. The lack of rate limiting made it easy for the attacker to attempt thousands of logins in a short period.
Recommendation: Enforce two-factor authentication for all admin accounts and implement rate limiting to prevent excessive login attempts. XML-RPC should be disabled by default or restricted to trusted sources only.
Action Item Owner: IT Security Team

Issue: The attacker had access to the compromised admin account for several days before any signs of content modification were noticed. This means that real-time monitoring and detection were not effective in spotting unauthorized access right away.
Recommendation: Implement an intrusion detection system to track unusual login activity and alert security teams immediately. Logs should be actively monitored for any suspicious changes in administrator accounts.
Action Item Owner: Cybersecurity Operations Team

Issue: The investigation took longer than it should have because log monitoring was not centralized, making it harder to quickly analyze all related events.
Recommendation: Use a centralized logging system to collect and analyze logs from all web applications and servers in real time. This will help speed up incident detection and response.
Action Item Owner: IT Administration Team

Conclusion

The breach was caused by a brute-force attack targeting XML-RPC, which allowed unauthorized admin access. The attacker modified the site's content and continued making changes for days

before being detected. The security team successfully removed unauthorized access, restored the site, and implemented stronger security measures.

To prevent future attacks, better authentication methods, monitoring tools, and stricter security policies are being put in place. With these improvements, similar incidents should be much less likely to occur in the future.