Overview

During my internship, I responded to a real malware incident on a WordPress site. The malicious PHP file displayed APT-style tactics including persistence, obfuscation, and potential privilege escalation. This case demonstrates detection, analysis, remediation, verification, and web application hardening.

Technical Environment

- **CMS:** WordPress
- **Hosting:** SiteGround
- **PHP Version:** 7.x/8.x
- **Tools:** SiteGround file manager, WordFence, browser devtools, grep search
- **Frameworks:** MITRE ATT&CK mapping, vulnerability management

Detection / Alert

- **Trigger:** Official SiteGround malware notification:

  “Malicious code was detected on newly uploaded/edited files that are part of your website. The permissions of the detected files were changed automatically to prevent further infection. Files must be cleaned within 3 days to avoid suspension.”

- **Malicious file location:** `/wp-content/plugins/wp-compat/wp-compat.php`

- **Alert Screenshot :**

SiteGround

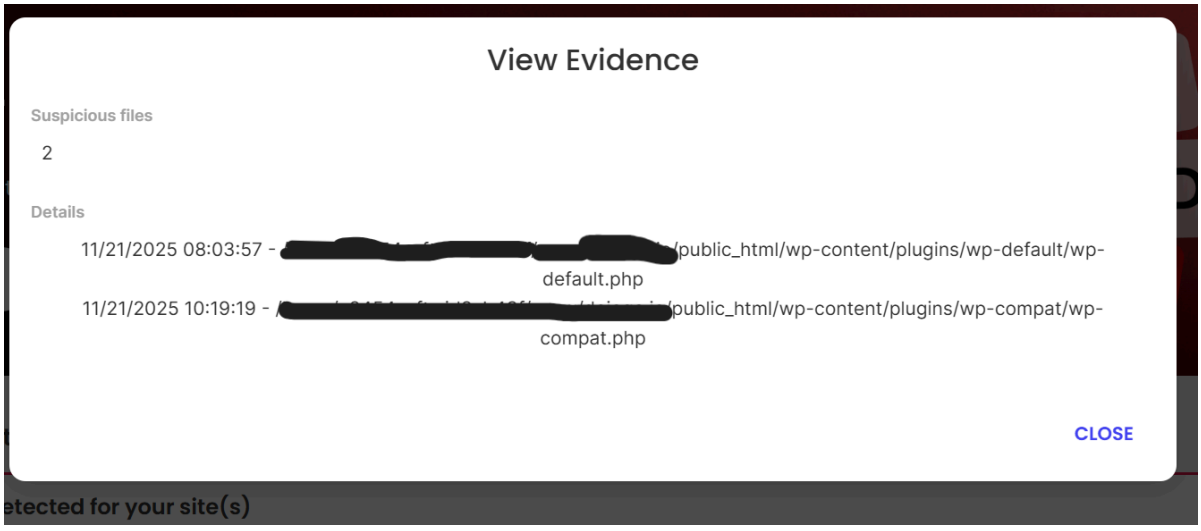
Dear [redacted]

We would like to notify you that a malicious code was detected on newly uploaded/edited files that are part of your website [redacted]. The permissions of the detected files have been changed and they are currently **not executable**. This is automatically done by our system to prevent further infection of your account. Please note that this is a temporary solution and **if the malicious files are not cleaned from your website within the next 3 days, we will have to suspend your website** since such files presence on our servers is a security risk.

More information on the case can be obtained from your Client Area > Home page > Important Notifications. There you will find a full security report with the exact location of the malware and instructions on how to clean up your website and avoid suspension.

Best regards,
The SiteGround Team

- **File Location Screenshot:**



Indicators of Compromise (IOCs)

- **New file inserted** in plugin directory
- File permissions temporarily changed by hosting provider
- Obfuscated PHP code (`eval`, `base64_decode`)
- Unauthorized admin-level actions logged
- **Malicious PHP Screenshot:**

[redacted]/public_html/wp-content/plugins/wp-default/wp-default.php

[redacted]public_html/wp-content/plugins/wp-compat/wp-compat.php

Analysis

- Identified persistent web shell with reinjection capability.
- MITRE ATT&CK Mapping:

Behavior	Technique
Obfuscated PHP web shell	T1505.003 – Web Shell
Persistence via plugin load hooks	T1547 – Boot or Logon Autostart Execution
Unauthorized admin access	T1078 – Valid Accounts
File modification & hiding	T1564 – Hide Artifacts

Remediation Steps

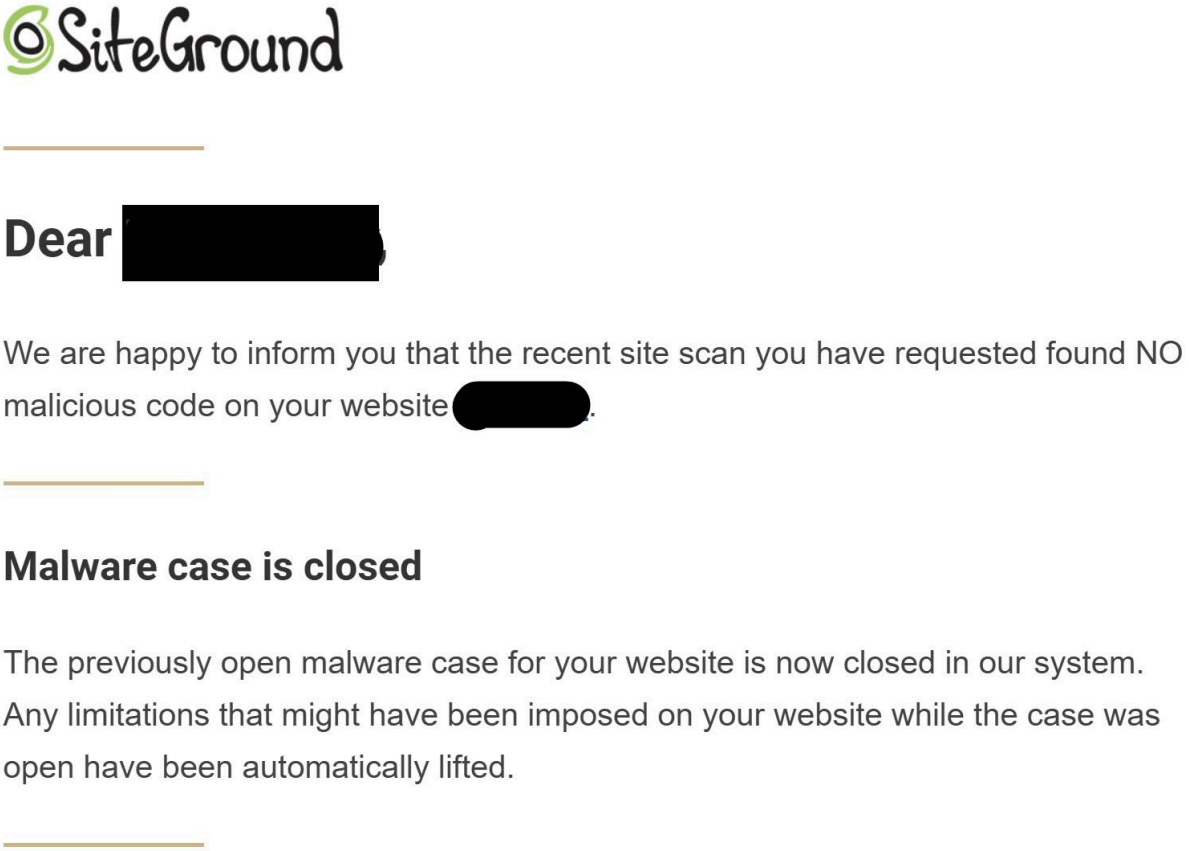
1. Activated maintenance mode
2. Full backup of files & database
3. Removed malicious plugin file & reinjection code
4. Verified plugin integrity
5. Updated WordPress core, plugins, themes
6. Reset admin credentials
7. Full scan for additional IOCs

Verification & Closure

- SiteGround scan confirmed:

  “We are happy to inform you that the recent site scan you have requested found NO malicious code on your website. The previously open malware case is now closed in our system.”

- **Screenshot:**


SiteGround

Dear [redacted]

We are happy to inform you that the recent site scan you have requested found NO malicious code on your website [redacted].

Malware case is closed

The previously open malware case for your website is now closed in our system. Any limitations that might have been imposed on your website while the case was open have been automatically lifted.

Hardening & Prevention

- Implemented plugin integrity monitoring and weekly scans
- Educated site owner on plugin hygiene and supply chain risks

Impact

- Complete removal of malicious PHP payload confirmed by hosting provider
- Restored site integrity & reduced attack surface
- Demonstrates structured incident response workflow: **detection → analysis → remediation → verification → closure**
- Skills highlighted: detection, analysis, remediation, verification, reporting, and security hardening

Lessons Learned

- Structured incident response is critical in real-world environments
- Mapping attacker behavior to MITRE ATT&CK improves analysis and reporting
- Automated alerts aid early malware detection
- Documentation and communication are essential in remediation