Web Service Incident and Hardening Review

Example report

Kit Baroness | Security analysis example

Assessment and source basis

My Security Incident Report analyzes a compromised website that prompted visitors to download a file and redirected them to another site. The supplied account links the compromise to an administrative account that retained a default password. The attacker reportedly changed website code and the administrative password, preventing the owner from signing in.

The work connects the reported customer symptoms to Domain Name System (DNS), HTTP, and TCP activity, then recommends limiting failed administrative sign-ins. The source describes sandbox capture, code review, and file analysis performed within the scenario. This review does not claim those tools were independently run again.

Evidence and analysis

These references identify the supplied report and its analysis sections. Original packet captures, source-code exports, and executable samples were not included for independent validation.

Source reference	Recorded observation	Supported reasoning
WEB-S1: customer reports	Visitors saw a download prompt, then redirection and slower computers after running a file.	The symptoms support investigation of an unwanted download and subsequent activity; user reports alone do not identify the payload.
WEB-S2: traffic analysis	DNS resolution and HTTP traffic to the original site preceded resolution and communication with another site.	The sequence is consistent with the reported redirection. Traffic order alone does not establish the executable's behavior.
WEB-S3: code and file analysis account	Added JavaScript prompted the download; the analyzed executable redirected visitors.	The supplied investigation links the code change and file behavior to the observed symptoms. Retain those underlying artifacts for confirmation.
WEB-S4: administrative access account	A default password enabled access; the attacker then changed the code and password.	Credential exposure and administrative control are the recorded contributing conditions.

Business effect and treatment

The immediate concerns are visitor exposure to malicious content, loss of control over the website, and interruption of administration. The record does not provide a measured number of affected visitors, financial loss, or a complete compromise timeline.

My primary recommendation was to limit repeated failed administrative sign-ins through controlled delay or account restriction. That should be implemented with monitoring and a recovery process so that protective controls do not create an unmanaged lockout risk. Replacing default credentials, using multifactor authentication, and reviewing administrative activity support the same objective.

Acceptance criteria

Proposed work	Proposed owner	Evidence required to complete
Restore trusted website content and administrative control.	Web service owner	Reviewed clean content, authorized administrative access, and checks that the unwanted prompt and redirect are absent.
Replace the default credential and strengthen sign-in controls.	Identity owner	Default access fails, approved access succeeds, repeated failures trigger the intended response, and recovery is checked.
Investigate affected traffic and files.	Security analyst	Preserved artifacts, documented findings, scope limitations, and follow-up decisions.

These are proposed validation conditions; completed implementation and retest results were not supplied. Close the review after service checks, retained evidence, and an accountable decision on remaining exposure.

Reference method

Incident analysis and recovery reporting are informed by NIST SP 800-61 Rev. 3. Access control and evidence-based validation can be tailored using SP 800-53 and SP 800-53A Rev. 5.

https://doi.org/10.6028/NIST.SP.800-61r3

https://doi.org/10.6028/NIST.SP.800-53Ar5