Incident Report

Case Title: Web Site Defacement – imreallynotbatman.com
Date of Report: 09/25/2025
Reported By: Security Operations Center (SOC)
Analyst: Nizar Aderbaz
Severity: High

1. Executive Summary

On **09/08/2016**, the SOC was alerted to a website defacement against the personal blog of the CEO of Dustin Yellin **(imreallynotbatman.com)**. Initial evidence was offered by the Gotham City Police Department (GCPD) in the form of a **Pastebin link** (http://pastebin.com/Gw6dWjS9) to the defaced content. An incident was investigated by the SOC using **Splunk** to identify the attack vector, attacker infrastructure, malware artifacts, and overall timeline of compromise. Proof confirms that the attacker exploited vulnerabilities in the web site's **Joomla CMS**, initiated a **brute-force attack** against administrative logins and, lastly, uploaded a defacement image and a malicious executable. Multiple attacker **IPs** and **domains** were found, with associated malware **hashes**.

2. Incident Timeline

Timestamp	Event
T0	Attacker (**40.80.148.42**) initiated scanning of victim website using **Acunetix** vulnerability scanner.
T1	Dynamic DNS domain **prankglassinebracket.jumpingcrab.com** resolved to **23.22.63.114** (used in pre-staging and brute force).
T2	Brute force attempts initiated against Joomla admin login. First password tried: `12345678.`
T3	**After ~412 password attempts**, correct admin credential identified: **batman**.
T4 (≈92 sec later)	Successful login confirmed.
T5	Attacker uploaded malicious executable **3791.exe** (MD5: **aae3f5a29935e6abcc2c2754d12a9af0**).
T6	Malware with SHA-256: **9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8** detected in spear-phishing campaign related to the compromise.
T7	Defacement file **poisonivy-is-coming-for-you-batman.jpeg** placed on web server. Website visibly altered.

3. Indicators of Compromise (IOCs)

IP Addresses

IP Address	Purpose / Context	VirusTotal (VT)	AbuseIPDB
40.80.148.42	Acunetix scanner (reconnaissance)	**51/72**	Not reported
23.22.63.114	Brute force & staging domain	**0/72**	1 report (3years ago)

Domains

Domain	Purpose / Context	VirusTotal	Talos Intelligence
prankglassinebracket.jumpingcrab.com	Malicious staging domain	**4/94**	**Untrusted / Malware site**

Malicious Files

File Name	Type / Context	Hash	VirusTotal (VT)
3791.exe	Uploaded executable	MD5: aae3f5a29935e6abcc2c2754d12a9af0	**64/72**
Spear phishing malware	Malicious payload	SHA-256: 9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8	**51/72**

Defacement File

- **poisonivy-is-coming-for-you-batman.jpeg**

Passwords Observed

- First attempted: **12345678**
- Successful: **batman**
- Total unique attempts: **412**

4. Attack Techniques (MITRE ATT&CK Mapping)

- **Reconnaissance (TA0043):** Vulnerability scanning with Acunetix
- **Initial Access (TA0001):** Brute force (T1110.001 – Password Guessing)
- **Persistence (TA0003):** Uploaded web shell/malicious executable
- **Impact (TA0040):** Website defacement (T1491 – Defacement)
- **Command and Control (TA0011):** Use of dynamic DNS domain

---

5. Root Cause Analysis

The compromise was made possible by:

1. **Weak administrative credential** ("batman") susceptible to brute force.
2. **Lack of account lockout policies**, allowing >400 attempts.
3. **Unpatched Joomla CMS** vulnerable to automated scans and exploits.
4. **Insufficient web application monitoring**, delaying detection until external notification.

---

6. Recommendations

1. **Credential Hardening**
   - Enforce strong password policies (minimum length, complexity).
   - Implement account lockout after defined failed attempts.
2. **System Patching**
   - Regularly update Joomla CMS and plugins.
   - Conduct vulnerability scans and patch high-severity issues promptly.
3. **Monitoring & Detection**
   - Enhance web server logging and integrate real-time alerting in SIEM.
   - Monitor brute force and unusual POST requests.
4. **Malware Protection**
   - Quarantine identified IOCs in endpoint detection solutions.
   - Share hashes/domains with threat intelligence platforms.
5. **Incident Response Procedures**
   - Establish playbooks for web defacement incidents.
   - Conduct tabletop exercises to ensure readiness.

---

7. Conclusion

The analysis confirmed that defacement of the web site was achieved through brute forcing **Joomla admin credentials** and then evil file upload. Attackers' infrastructure **(IPs, domains, hashes of malware)** was also mapped and a full timeline of the incident reconstructed. Improved deployment of tighter credential policies, patch management, and careful monitoring would have prevented or lessened this incident's impact.