# Cyber Challenge Incident Response Report

| | |
|---|---|
| Incident Name | **Critical website hack (possible leaked customers' personal data)** |
| Report Team | Ricardo Amano Torres<br>Jesús Eduardo Ramírez Mejía<br>César Rivera<br>Héctor Alejandro Canizales Pena |
| Report Date | **July 12th, 2021** |
| Externship Program | **PrepaTec Cybersecurity** |

## Executive Summary

Complete the three sections below with your key observations and takeaways related to the intrusion. In this report you will:

- Explain the adversary's tactics, techniques and procedures.
- Outline the most significant courses of action taken to defend against the adversary when responding to the intrusion.

The National Institute of Standards and Technology (NIST) Special Publication NIST 800-61, Computer Security Incident Handling Guide, provides advice on prioritizing the handling of security incidents. These incidents may be applicable to computer systems as well as paper or other media. Per NIST 800-61, section 3.2.6 (Incident Prioritization) relevant factors for event threat and impact/escalation criteria include:

- Functional Impact. Incidents targeting IT systems typically impact the business functionality that those systems provide, resulting in some type of negative impact to the users of those systems.
- Information Impact. Incidents may affect the confidentiality, integrity, and availability of the organization's information.

**Examples of FUNCTIONAL impact categories**

| Category | Definition |
|---|---|
| **None** | No effect to the organization's ability to provide all services to all users. |
| **Low** | Minimal effect; the organization can still provide all critical services to all users but has lost efficiency. |
| **Medium** | Organization has lost the ability to provide a critical service to a subset of system users. |
| **High** | Organization is no longer able to provide some critical services to any users. |

**Examples of possible INFORMATION impact categories**

| Category | Definition |
|---|---|
| **None** | No information was exfiltrated/leaked, disclosed, changed, deleted, used, or disclosed by or for unauthorized persons or purposes, or otherwise compromised. |
| **Privacy Breach** | Sensitive personally identifiable information (PII) of employees, etc., was accessed or exfiltrated/leaked, or protected health information (PHI) of individuals was used or disclosed by or for unauthorized persons or purposes, or otherwise compromised. |
| **Proprietary Breach** | Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed, exfiltrated/leaked, or used or disclosed by or for unauthorized persons or purposes. |
| **Integrity Loss** | Sensitive or proprietary information was changed or deleted accidentally or intentionally. |

# Section I: Triage [Complete BEFORE incident response]

The objective of the triage process is to gather information, assess the nature of an incident and begin making decisions about how to respond to it. It is critical to ensure when an incident is discovered and assessed the situation does not become more severe.

1. **What type of incident has occurred?**
    a. A buffer overflow attack was executed using vulnerability CVE-2019-11043 which in turn produced remote code execution, provoking files to be added to the web server, especially changing Joe's catalog for a malware in Adobe Acrobat (CVE-2008-2992) and possibly adding a backdoor.
2. **Who is involved?**
    a. Hacker going by the alias of **Hax0r**
3. **What is the scope?**
    a. Narrow, only users who visit this website or access to the pdf catalog might be compromised.
4. **What is the urgency?**
    a. Medium
5. **What is the impact thus far?**
    a. A malicious pdf file containing malware was copied to the web server and is downloadable by end users.
    b. Compromised purchases
6. **What is the projected impact?**
    a. There could be a privacy breach on most of the customers who have downloaded and opened the malware pdf catalogue file. Most of their personal information, accounts, and passwords could have been sent to a server and sold for big money.
    b. Back doors (and/or rootkits) could have been installed into the server (but haven't been found as of now)
7. **What can be done to contain the incident?**
    a. Shut down the web server
    b. Update nginx and php to their latest versions and verify that there aren't any vulnerabilities present (CVEs) in their software
8. **Are there other vulnerable or affected systems?**
    a. https://www.kb.cert.org/vuls/id/593409/ (Explanation of Adobe Acrobat CVE-2008-2992)
    b. Yes, if the customers download and open the file through "Adobe Acrobat and Reader 8.1.2" hackers may be able to execute arbitrary code as per CVE-2008-2992.
9. **What are the effects of the incident?**
    a. Arbitrary code can be called when opening a PDF file. Thus, possibly compromising all customer files, accounts, and passwords.
10. **What actions have been taken?**
    a. Analyzing the contents of the pdf file, it was found that it's a malware which uses a CVE regarding Adobe Acrobat reader.
    b. We made up a new rule for identifying any other attack from Hax0r with a YARA rule
11. **Recommendations for proceeding?**
    a. Shut down the web server

b. Notify all customers to update to the latest version of Adobe Acrobat and Reader, at least v8.1.3

c. Tell customers to change all their passwords and check any suspicious spending of their bank accounts or any account passwords /emails that may have been stored in their computers.

d. Add 2FA, maybe self-host a password manager and suggest employees to use it.

e. Segment the network, create authentications between the segmented servers.

f. Perform pen testing into the network as well as phishing attacks to test employees’ training.

**12. May perform analysis to identify the root cause of the incident?**

a. yes

## Section II: The Adversary’s Actions and Tactics [Complete DURING the incident response]

As far as we know, Hax0r wanted to gain administrator privileges of the website and access customer data through malware covered as a PDF document. Until now, Splunk has recorded 35 errors at logging as administrator and helped us to uncover Hax0r’s IP address, but hasn’t done great damage to the web server so far. However, it was able to upload possibly harmful files to the server and this might affect customers that may download them on their devices.

### Description of the Adversary

The adversary evidently is experienced in cybercrimes and has the knowledge to access systems, he or she may have tried to gain access to systems of other companies or targets.

Describe observations and indicators that may be related to the perpetrator of the intrusion. If possible, highlight the attributes of the adversary operator and the adversary’s potential customer. Outline potential motivations and identifying elements.

**Apparently, Hax0r is a person who has access to programs to exploit servers and propagate malware with social engineering. It may also have a good data theft history from which he finds clients and develops more sophisticated attacks.**

### The Adversary’s Capabilities

Describe the adversary's capabilities in terms of tactics, techniques and procedures (TTPs). Address the tools and tradecraft employed by the intrusion perpetrators, such as exploits backdoors, staging methods and situational awareness.

Describe the infrastructure, such as IP addresses, domain names, program names, etc. used by the adversary.

IP address: 60.163.119.242

Domain names:

- retro.lab/ | Joe Averaggi's retro websites
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11043 (PHP vulnerability)
-

Program names:

- Adobe Acrobat Reader https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2992 (Adobe Acrobat Reader vulnerability)
- Programming languages such as Python to exploit the PHP vulnerability
- File hosting service or web server such as nginx to host the pdf file so that the remote code execution vulnerability could download the file.

## Section III: Root Cause Analysis [Complete AFTER the incident response]

The Computer Security Incident Handling Guide (NIST 800-61) provides advice on event analysis activities**.**

1. **Exactly what happened, and at what times?**

Hax0r tried to remotely control the server between 8:39 p.m. and 8:41 p.m.

**2. How well did staff and management perform? Were documented procedures followed? Were procedures adequate?**

As far as we know, after the reports of some clients that the catalog file was being tagged as malicious the cybersecurity team (us) was called. So apparently no ation had been taken by Joe. DataGrid might have done a good job as Hax0r didn't gain admin privileges on the server.

**3. What information was needed sooner?**

The fact that an unwanted actor had temporary access - including remote code execution- to the server, as well as the fact that potentially important files had been changed.

**4. Were any steps or actions taken that might have inhibited the recovery?**

The fact that the server used a strong password when connecting through SSH might have made the attacker back off and stop trying to brute-force an SSH connection.

**5. What would/should staff and management do differently the next time a similar incident occurs?**

Check the source of the attack to verify it's not from the same hacker
Verify files each time they are downloaded

**6. How could information sharing with other organizations have been improved?**

Reporting to MITRE and other vulnerability oriented companies that some reported vulnerabilities have been used in real-world attacks.

**7. What corrective actions can prevent similar incidents in the future?**

Keeping software up to date,
Researching possible vulnerabilities based on the software that is used on the web server

**8. What precursors or indicators should be watched for in the future to detect similar incidents?**

Hash algorithms should be performed on a regular basis to identify any critical software or files that have changed (when they aren't supposed to).

**9. What additional tools or resources are needed to detect, analyze, and mitigate future incidents?**

Splunk,
The YARA rule can be useful to detect attacks by the same hacker (Hax0r).