WEBSITE DEFACEMENT

MAY 2020

ITSAP.00.060

This document introduces **website defacement**, which is a form of cyber attack on your website. Think of web defacement as virtual graffiti or vandalism. A hacker defaces a website by changing its appearance or content. Threat actors may be motivated to deface a website for various reasons, ranging from attempting to embarrass website owners or promoting alternative views. In some cases, a threat actor may deface a website by injecting malicious code that infects visitors' devices. Read through this document to learn how to protect your website against this type of attack.

HOW ARE WEBSITES DEFACED?

Hackers use different methods to deface websites. Typically, hackers inject infected code into the site's script, which allows them to take control of the website. With this control, they can gain access privileges to the website and any sensitive content. When defacing a website, hackers may use a virtual private network (VPN) for anonymity. Using automated scanning software to find website vulnerabilities, attackers can access the website through a break in the program (e.g. a vulnerability). Hackers can be disguised as authorized users, accessing remote files on websites to execute their own commands.

WHY ARE WEBSITES DEFACED?

Hackers may deface a website for personal and political motivations. There are many reasons why attackers compromise or deface websites. Some examples include the following:

- Social and political motivations (e.g. protesting a specific movement ["hacktivists"]).
- Traffic generating profit (e.g. redirecting traffic to commercial or infected websites to make profit or exploit targets).
- Bandwidth or computing resource piracy (e.g. spreading automated attacks).
- Private data theft (e.g. stealing customer information).
- Ego: Personal enjoyment or challenge (e.g. taunting website owners by exploiting vulnerabilities).

WHAT DO I DO IF MY WEBSITE IS DEFACED?

Do not panic if your website is defaced; threat actors are looking for a reaction (e.g. attention, fear). If an attack takes place, follow these steps to restore your website:

- Contact the vendor, if you have a vendor-hosted website, to report any abnormal activities.
- Replace the website with a maintenance page immediately.
- Inspect the contents and latest back-ups of the site for hidden malware and vulnerabilities.
- Inform relevant parties of the incident (e.g. customers, suppliers, third parties).
- Make a statement to the public to preserve your organization's reputation.
- Restore your website with back-ups to ensure quick recovery.
- Report the incident to the police.
- Have technical support analyze how the website was defaced and evaluate the process of response (e.g. to improve for any future complications).

HOW DO I SELECT A VENDOR TO HOST MY SITE?

If you are thinking of hosting your website through a vendor, ask the following questions to identify the measures that the vendor has in place to plan for, respond to, and recover from website defacement.

PLAN

- What security procedures does the vendor have in place?
- How frequently does the vendor run back-ups, and where are they stored?
  - Back-ups should be kept away from their main sever and in a secure location to ensure that a clean system restore is an option.
  - A history of back-ups should be considered to determine whether a previous back-up can be restored, depending on the state of the latest version.
- What kind of technology or tools are used to stop intrusions (e.g. firewalls and Secure Sockets Layer [SSL])?

RESPOND

- How often does the vendor monitor the network for unauthorized activity?
  - If malware is detected early enough, it can be stopped before it spreads (e.g. running antivirus and malware scans).
  - Reports for these scans should be accessible.
- Does the vendor have incident response plans and procedures to assign specific administrators to respond to incidents?
- How is administrator access controlled?
  - The number of admin accounts should be limited.
  - Multi-factor authentication should be used.
  - Administrators should undergo security screening before access is implemented.

RECOVER

- What is the projected timeline for the website to be restored if an attack takes place?
  - A maintenance page should be prepared and ready for use.
  - Consider a service level agreement entry for restoration time.
- How long are the audit reports retained for review and analysis (e.g. duration o keep track of potential repeating threats)?
- Does the vendor know how to deal with emergent threats (e.g. vulnerabilities that might be exploited before a patch is available)?
- What are their procedures to avoid social engineering attacks (e.g. threat actor calling to request a change in the data)?
- How do they protect data through routers and switch security to ensure attacks do not get through?
- Is the data encrypted, and are the encryption keys secure?
  - Encryption keys should not be stored within the data. They should be stored by the tenant organization or a third-party contributor.

HOW DO I PROTECT MY SELF-HOSTED WEBSITE?

If you are using a self-hosted website, you should also consider these security tips to help protect your website from defacement:

- Use passphrases or strong passwords to keep threat actors from having easy access through default log-in credentials.
- Manage access for user accounts and minimize privileges on administrator accounts (e.g. delete users who leave the organization or no longer need specific access).
- Identify a point of contact (and a back-up) for incident response.
- Train employees on incident response procedures.
- Use a firewall to flag and block malicious traffic.
- Use monitoring and detection tools to track unauthorized changes to your website.
- Back up your database regularly and before performing updates.
- Update plug-ins to fix bugs and patch security issues.
- Install updates and patches on your website server.

Security should be considered when designing and developing your website. Work with your development team to ensure that they are trained on security and secure coding practices, such as the following examples:

- Encoding outputs (e.g. HTML and URL outputs) properly to prevent cross-site scripting attacks.
- Using specific coding alternatives (e.g. third-party library) to protect the website from Structured Query Language (SQL) attacks.
- Using HTTPS-only cookies to protect your website from hackers who are trying to access user credentials.
- Protecting server-side code from being downloaded.

You may want to work with a security specialist who can help you evaluate the security level of your system and identify further ways to protect your website, such as conducting vulnerability scans or penetration tests.

The Open Web Application Security Project (OWASP) is a not-for-profit organization that has educational resources, guidelines, and open source tools that you can use to improve the security of the software you use. For more information, visit the OWASP website: **https://www.owasp.org/**

Need help or have questions? Want to stay up to date and find out more on all things cyber security? Come visit us at the Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**