Website defacement

February 2024

ITSAP.00.060

Website defacement 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 to promoting alternative views. In some cases, a threat actor may deface a website by injecting malicious code that infects visitors' devices. This guidance can help you learn how to protect your website against this type of attack

How websites are 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. Attackers can use automated scanning software to find website vulnerabilities. They can then access the website through a break in the program, such as Structured Query Language (SQL) injection or cross site scripting. Hackers can also be disguised as authorized users, accessing remote files on websites to execute their own commands. Refer to Virtual private networks (ITSAP.80.101) to learn more.

Why websites are defaced

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

- social and political motivations, such as protesting a for specific movement, also known as hacktivists
- opportunities to make a profit or exploit victims by redirecting traffic to commercial or infected websites
- bandwidth or computing resource piracy, such as spreading automated attacks
- private data theft, such as stealing customer information
- ego: personal enjoyment or challenge, such as taunting website owners by exploiting vulnerabilities

What to do if my website is defaced

Do not panic if your website is defaced, threat actors are looking for a reaction. 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, such as customers, suppliers and third parties
- make a statement to the public to preserve your organization's reputation
- restore your website with backups 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

AWARENESS SERIES

Cat. No. D97-1/00-060--2024E-PDF
ISBN 978-0-660-70412-8

How to select a vendor to host my website

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 backups, and where are they stored?
  - Backups should be kept away from their main server and in a secure location to ensure that a clean system restore is an option
  - A history of backups 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, for example, firewalls and Transport Layer Security (TLS)?

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 by running software such as anti-virus 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
  - Use multi-factor authentication (MFA) on all accounts, where possible
  - Conduct security screening for administrators before access is implemented

Recover

- What is the projected timeline for the website to be restored if an attack takes place?
  - Prepare a maintenance page
  - Consider a service level agreement entry for restoration time
- How long are the audit reports retained for review and analysis? For example, should you keep them to monitor potential repeating threats?
- Does the vendor know how to deal with emergent threats? For example, whether there are vulnerabilities that might be exploited before a patch is available?
- What are their procedures to avoid social engineering attacks, such as threat actors calling to request a change in the data?
- How do they protect data through router 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 to protect your 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. For example, delete users who leave the organization or no longer need specific access
- identify a point of contact and a backup for incident response
- train employees on incident response procedures
- use monitoring and detection tools, like and intrusion prevention or intrusion detection system, to identify malicious activity and 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:

- encoding outputs, like HTML and URL outputs, properly to prevent cross-site scripting attacks
- using specific coding alternatives, like third-party library to protect the website from **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
- use an intrusion prevention system (**IPS**) to monitor malicious activity

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. Examples include, 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 to help you improve the security of the software you use. .

Learn more

- Domain name system (DNS) tampering (ITSAP.40.021)
- Network security logging and monitoring (ITSAP.80.085)
- Security considerations for your website (ITSM.60.005)
- Tips for backing up your information (ITSAP.40.002)
- Managing and controlling administrative privileges (ITSAP.10.094)
- Steps for effectively deploying multi-factor authentication (MFA) (ITSAP.00.105)
- Top 10 IT security actions: #6 provide tailored cyber security training (ITSM.10.093).
- Top 10 IT security action items: No.2 patch operating systems and applications (ITSM.10.096)