National Cyber Security Centre
Ministry of Security and Justice

Help! My website has been defaced

What can you do to prevent defacements?

Factsheet FS-2015-01
version 1.0 | 11 May 2015

To deface a website an attacker changes the content of existing pages or adds new ones. Hundreds of websites are defaced every day, often without being specifically targeted.

It is becoming increasingly common for defacements to leave behind malware, which may infect visitors to the website. It is therefore important to adequately prepare the resolution of and the communication regarding defacements.

Many websites are vulnerable to easily preventable defacements. There are various measures you can put in place to substantially reduce the risk of a defacement.

This factsheet sets out the key characteristics of a defacement, what implications they have and what you can do to maximize your defence against such attacks.

Target audience
This factsheet is intended for website owners, developers, and administrators.
When you own a website but have outsourced its development and/or management, you should consult with your suppliers about how you can collaborate to prevent this type of abuse.

Produced in partnership with **SIDN** and **AIVD**.

Key facts

» When an attacker changes the content of a website that is called a defacement.
» Defacements occur frequently, and usually follow an attack on your CMS or web server.
» Attackers use defacements to spread malware.
» The risk of defacements can be reduced by properly managing and securing websites.
» A well-prepared response makes it possible to recover from a defacement more quickly.

What is defacement?

To deface a website, an attacker changes the content of existing pages or adds new ones. The defacement may be very obvious, or concealed. A defacement often follows an attack on a CMS[1] or web server, e.g. by abusing a vulnerability or an existing user account and password.

Defacements may target a specific organization, but in the vast majority of cases they are untargeted. Untargeted, automated defacements can modify a large number of websites in one go. Hundreds of defacements take place every day, all over the world[2].

Defacements can also be carried out discreetly. An attacker could add or modify a single article on a news site so that it takes a while before anyone notices the change and the message is more likely to be conveyed. Also, a defacement can turn a website into a distribution point for malware.

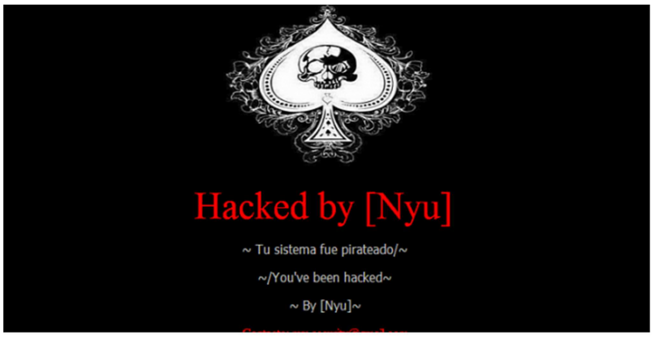
There may also be other ways of presenting a website visitor with the wrong information, for example through a DNS hijack[3]. With a DNS hijack the user, when requesting a certain website, is directed to a false page. Although this is not 'formally' classified as a defacement, it may have similar implications[4].

[1] A content management system (CMS) is software that is used to manage the content of a website. Examples of commonly used CMSs include Joomla!, WordPress and Drupal.
[2] www.zone-h.org registers between 50,000 and 100,000 website defacements a month.
[3] Domain Name System, the online service that translates a domain name (such as www.ncsc.nl) into the accompanying IP address.
[4] For an example, see: http://www.esecurityplanet.com/hackers/hackers-deface-malaysia-airlines-website.html

Who carries out defacements and why?

Hackers, script kiddies and cyber vandals often carry out defacements just ‘because they can’. They run programs to scan the internet in search of vulnerable websites and replace the home page with a page of their own in what we refer to as a 'mass defacement'.

This form of defacement is a kind of digital graffiti in which the hacker leaves behind his 'tag'. On the internet there are ranking lists that are kept to show how many websites an individual has hacked. Each successful defacement enhances his image.



Hacked by [Nyu]

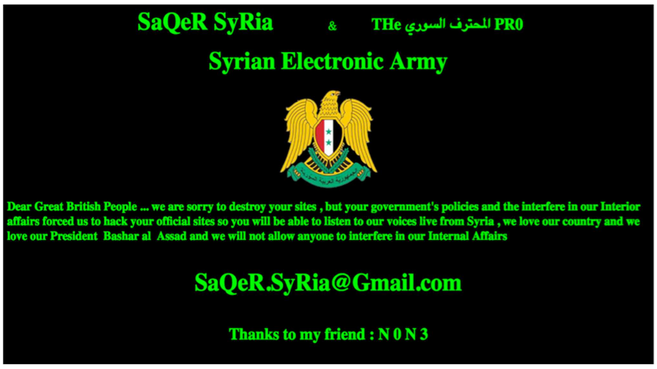
~ Tu sistema fue pirateado/~

~/You've been hacked~

~ By [Nyu]~

1 Example of a *tag*.

Hacktivists such as Anonymous or hacker groups like the Syrian Electronic Army carry out defacements to communicate their ideological message or to sabotage opponents.
In many cases they set out to deface as many websites as possible in a certain country or of a certain type of organization in order to spread their ideological message.



SaQeR SyRia & THe المحترف السوري PR0

Syrian Electronic Army

Dear Great British People ... we are sorry to destroy your sites , but your government's policies and the interfere in our Interior affairs forced us to hack your official sites so you will be able to listen to our voices live from Syria , we love our country and we love our President Bashar al Assad and we will not allow anyone to interfere in our Internal Affairs

SaQeR.SyRia@Gmail.com

Thanks to my friend : N 0 N 3

2 Example of an ideological defacement.

Cyber criminals in pursuit of financial gain modify websites to distribute malware, steal login details or to connect them to a botnet. Here too, the perpetrator will try to do this discreetly so the site remains compromised for as long as possible. Another growing phenomenon involves placing malware-infected advertisements on bona fide websites.

Finally, there are cases where disgruntled former employees maliciously deface the website of their past employer. They are able to do this because they still have the information such as user names and passwords that they need to easily modify the website.

How serious is a defacement?

The implications of a defacement may differ between organizations. Organizations have to assess the potential impact of a defacement themselves and take appropriate measures. The initial impact of a website being defaced usually takes the form of the company's image being damaged and the costs involved in restoring the website. Companies that depend on their website for their business operations may also suffer financial losses owing to reduced sales.

A website defacement will generally not affect an organization's underlying computer systems, but could be used as a diversion for other forms of cybercrime. Cyber criminals may also use defacements as a way of obtaining employees' login details for an organization's webmail system, making use of the organization's domain name for this purpose.

If a defacement is used to spread malware or to induce visitors to a website to enter their login details for the site or authentication services such as Facebook, Google or DigiD, the damage goes beyond the impact it has on the affected company. In such cases the personal information of visitors or company information may be misappropriated.

What makes me vulnerable?

A website is vulnerable to defacements if:

» the (virtual) web server or the VPS-interface[5] is not securely configured. If unauthorized persons are able to gain access to the web server or the VPS it is possible for them to add content or to modify or delete it;

» the CMS (or CMS plugins) contains vulnerabilities. Most CMS suppliers regularly publish security updates for their products in order to resolve newly detected vulnerabilities;

» the login details for the CMS or the web server have fallen into the hands of attackers, e.g. by making use of standard accounts and passwords, through targeted phishing emails[6] or if the website does not make use of TLS[7] to exchange confidential information;

» the website configuration contains vulnerabilities such as XSS[8], that can be used to present 'false' content;

» malware is placed on the website by unreliable advertisement suppliers.

[5] Virtual private servers (VPS) can be used to create several logically separated virtual servers on a physical web server.

[6] Phishing emails are misleading emails containing a link to a false website or which contain malicious software.

[7] TLS – Transport Layer Security, a protocol for setting up and using a cryptographically secured interface between two computer systems. For more information see https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html.

[8] Cross Site Scripting (XSS) is an attack method that can be used (among other things) to present false content to a user. See also https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29.

The websites of certain types of organizations, such as religious and political organizations and media companies, are especially at risk to targeted attacks. But website defacement of organizations such as these does not necessarily indicate a targeted attack, and there remains a good chance that the affected website is one of the victims of a mass defacement.

Defacement of social media

It is important for organizations using social media such as Twitter and Facebook to consider the implications of these services being abused. False messages on Twitter or a modified Facebook profile could harm your image as seriously as a website defacement.

There is little that you as a user can do to improve the security of large social media sites, but you can protect yourself as effectively as possible against having your user account abused:

- Use 2-factor authentication wherever possible.
- Regularly change your passwords, also when people with access to them leave the organization.
- Formulate a response plan.

How do I notice a defacement?

Most defacements are so obvious that there is no doubt that the site has been defaced and who is claiming responsibility for it. There are various technical measures you can take to monitor your website for unauthorized changes. There are also companies that will do this for you for a fee.

If you do not immediately notice a defacement, you may be alerted by:

- users who visit the site and notice the defacement;
- online databases that register defacements and, in some cases, send a message to the site administrator;
- monitoring public comments on your website on social media such as Twitter;
- your internet service provider, which is often the first to be alerted if your website is abused.

How do I prevent a defacement?

Although it is never possible to entirely rule out the chance of your website being defaced, there are various preventive measures you (or your supplier) can take to substantially reduce the risk.

- Make sure that you have a robustly configured server on which no unnecessary services have been installed.
- Always install the latest patches and security updates on your system.
- Regularly check that your system is still up-to-date and also check it for the presence of malware.
- Do not use standard accounts and passwords for your operating system or CMS.
- Immediately delete the user accounts of employees who leave the organization or no longer need access to the CMS or web server.
- Install a firewall and filter the network traffic for suspicious patterns.
- Limit the number of IP addresses that can gain access to the web server and CMS.
- Only access the CMS via a secure TLS connection.
- Where possible, secure access to the web server and the CMS with a 2-factor authentication system[9].
- Regularly scan the site's security level, using automated scanners for instance. Arrange this beforehand with the website's administrators or owners so that this is not seen as an attempted attack.
- Introduce a responsible disclosure policy[10] so that vulnerabilities found in your website can be confidentially reported. That will make it possible for you to correct these vulnerabilities before they are abused by others.
- If your website is hosted by an external supplier, make clear agreements on the website’s security.

Additionally, and certainly if the website or the image of the organization is especially important or there is an above-average risk of defacement, you could consider:

- periodically performing a penetration test[11] on the quality of the security of the website and repairing any detected vulnerabilities. This way you can detect the XSS vulnerability touched on above;
- implementing an Intrusion Detection System (IDS)[12] to detect suspicious activities sooner.

How do I prepare myself for a defacement?

Since there is no such thing as a 100% safety guarantee, you must always be prepared to limit the damage caused by a defacement.

- Regularly make a backup of the site. This will make it easier to repair the site.
- Makes sure that you have a presentable substitute web page that can replace the defaced website immediately.
- Formulate a response plan setting out what to do in the event of a defacement (see the paragraph below). You should also consider the internal and external communication on the incident.
- If the website is hosted by an external supplier, make clear agreements in advance on what the supplier may/should do on his own initiative and what has to be discussed with the client first.

[9] With 2-factor authentication a second means of authentication, such as an SMS verification code, is used in addition to a password.

[10] For more information see: https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html

[11] For more information see https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/pentesten-doe-je-zo.html.

[12] For more information see https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/intrusion-detection-system.html.

The most important measures against a defacement

Prevention:

1. Make sure that your web server and CMS are securely configured and always install the latest security updates.
2. Where possible, use 2-factor authentication for access to your web server and CMS.

Preparation:

3. Regularly make a backup of your site.
4. Formulate a response plan setting out what to do in the event of a defacement.

Repair:

5. Place a substitute web page.
6. Internally and externally communicate the incident and the possible implications.
7. Secure the compromised content for criminal investigation purposes and report the incident to the police.
8. Reconfigure your website and carefully check the security settings before putting it back online.
9. Look into where you can improve the configuration or management of the site or the incident response and carry through the improvements.

How do I repair a defacement?

The formulated response plan is put into effect as soon as a defacement is established.

To ensure a quick repair, it includes:

- Placing a presentable substitute web page.
- Establishing the damage caused by the defacement. Is it only the site's appearance that has been changed, or has the attacker has also left malware or illegal content behind?
- Inform relevant parties of the incident.
- Secure the content and the logging of the attacked site for criminal investigation purposes.
- Try to find out how the defacement was carried out, which vulnerabilities were abused.
- Check the most recent backup of the site for the presence of malware and vulnerabilities.
- Set up a new server with the latest versions of the necessary software and place the most recent, secure backup of the site's content on it.
- Publish the newly configured site as soon as it is clear that all vulnerabilities have been resolved.

Once the website has been repaired there remains plenty to be done to make sure that there is no recurrence:

- Always report the incident[13] to the police.
- Establish whether the site is still subject to any technical vulnerabilities. Repair them or rebuild the website with less vulnerable products.
- Look into whether any improvements can be made to how the site is managed. In this context you could consider the timely installation of patches and updates, the monitoring of your site and the organization's response to the incident.
- If you manage the website yourself or are dissatisfied with the options provided by your current supplier, consider changing the hosting to another supplier.
- Evaluate the response plan. What went well, and where is room for improvement? Should the response plan be tested (more often) in the future? Are more or fewer measures required?
- Once you have identified structural improvements based on the above, take an active approach to implement them.

Finally

Website defacements are being used increasingly as a propaganda tool for ideological groups. Also, more and more instruments are being produced to automatically scan websites and modify them automatically if vulnerabilities are found.
By taking specific security measures you can substantially reduce the risk of a defacement.

To make organizations less vulnerable to these and other attacks the NCSC has published (in Dutch) the 'ICT-beveiligingsrichtlijnen voor webapplicaties'[14].

More factsheets and guidelines on the protection of websites are provided at https://www.ncsc.nl:

- IT security guidelines for Transport Layer Security (TLS);
- Factsheet Help! My website is vulnerable to SQL injection;
- Factsheet HTTPS could be a lot more secure.

[13] For more information see https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/handreiking-cybercrime.html
You can also report an ideological defacement to the Dutch General Intelligence and Security Service (AIVD): www.aivd.nl.

[14] For more information see https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

Publication of **National Cyber Security Centre**
Turfmarkt 147 | 2511 DP The Hague | The Netherlands
P.O. Box 117 | 2501 CC The Hague | The Netherlands
www.ncsc.nl/english | info@ncsc.nl | T +31 (0)70-751 55 55
Publication No. FS-2015-01 v.1.0 | No rights may be derived from this information.