Server side alerts

Malware

Definition

Malware is short for "malicious software". In Nimbusec, malware usually refers to viruses, worms, trojan horses, Java script exploits and many other types of software that aim to compromise a website visitor's computer.

How is it detected

When Nimbusec visits a website, all data received is analysed with multiple commercial and open source anti virus engines. If any of those engines report suspicious data, Nimbusec raises an alert.

Alert levels

- *RED*: Identification of known malware based on signature
- *YELLOW*: Identification of unknown malware based on behavior analysis or open source antivirus engine.

Recommended action

Act fast! Your website visitors are being attacked right now. This represents a major legal and reputational risk for you. Please consider to put your website into maintenance mode right away. Nevertheless, before attempting to clean up your site: Backup your entire webspace and database. Determine what part of your website was responsible for distributing malware. Often malware is distributed through advertisement banners, javascript attacks or compromised downloads. Nimbusec will tell the URL of detected malware. Use this as starting point for your analysis. If you cannot determine the problem yourself, ask an IT forensics expert for help. You can find additional information at (StopBadWare.org)https://www.stopbadware.org/my-site-has-badware

Webshell

Definition

A webshell is a script that can be uploaded to a web server to enable remote administration of the machine. Webshells are usually found by Nimbusec's Server Agent. This result is in many ways similiar to the Malware result type, except that it contains more information and it's paths are file paths. You can find more information about webshells at the (US CERT)https://www.us-cert.gov/ncas/alerts/TA15-314A

How is it detected

- Nimbusec Server Agent analyse source files based on behaviour patters and signature database or
- Nimbusec External Scan analyse public files based on antivirus engines, behaviour patters and signature database

Alert levels

- *RED*: Identification of known malware/webshells based on signature
- *YELLOW*: Identification of unknown malware/webshells based on behavior analysis

Recommended action

Webshells often stay inactive for weeks before they create damage. Even so, they are usually able to deface a website completely or abuse your webserver's ressources. Before attempting to clean up your site: Backup your entire webspace and database. Investigate the indicated file, related log-entries and remove malicious code. Start forensic analysis for vulnerabilities that allowed malware to be placed based on file meta-data and log entries. Often outdated web applications (e.g. CMS systems) are exploited for malware placement.

Configuration

TLS

Definition

We perform several checks on the TLS protocol and certificates to ensure the traffic to the website is really secure. Checks:

- Certificate expiring date: We check the expiring date of a certificate and warn before it will expire and create warnings for customers or breaks tools relying on that certificate.
- Certificate expired: Worst case, but happening. If a certificate expired already we notice that.
- Unsafe ciphers: based on recommendations of international security companies
- Insecure protocol usage

Details on specifics like ciphers can be found in our FAQ section here.

How is it detected

It is detected via the nimbusec Cloud Scan.

Alert levels

- *RED*: An unsafe configuration was detected and should be handled immediately.
- *YELLOW*: Whatever it is, it can cause trouble in the near future and should be considered to be fixed soon.

Recommended action

Update, renew your TLS certificate if it is about to expire or allows use of unsafe configuration.

Update server configuration if possible to e.g. SSL/TLS Deployment Best Practices.

Application

Definition

This scan tries to detect installed applications, content management systems (CMS), webservers and used software. This information, a large knowledge base on software versions and Common Vulnerabilities and Exploits (CVE) databases is used to give information about possible vulnerable and exploitable software on a webserver through a website and if software, especially CMS is outdated and in need of an update.

How is it detected

- Nimbusec Server Agent detects the five most used CMS in any version.
- Nimbusec Cloud Scan tries to detect any application visible from the outside.

Alert levels

- *RED*: Software was found which is potentially attackable. This means a CVE is known with a high rating or a public available exploit.
- *YELLOW*: Outdated software was found, as well as low public CVE entries.

Recommended action

In case of an outdated and vulnerable software, update it to the most recent version.

- Delete plugins and themes that are not needed
- Update always to the most recent version to fix vulnerabilities
- Care about safe passwords and
- Access permissions to your systems

Sometimes an update cannot be performed. On first sight that is not a problem, just have a closer look at the specific website. Maybe the software vendor has patches for this specific version to fix some security flaws. At least monitoring can be upgraded to a faster interval, in case something happens, the first one to know is the website owner.

Downloadable Sources

Definition

Downloadable software is suspected to be accessible from the outside and may contain passwords or other confidential information that can be used to compromise the webserver or to make a public statement or to leak information. This can be for example:

- forgotten database dumps (db.dmp, mysql.bkp, ...)
- temporary configuration files (configuration.php.tmp, config.php.sample, ...)

How is it detected

It is detected via the Nimbusec Server Agent.

Alert levels

- *YELLOW*: We found suspicious files, but did not check availability from external yet.

Recommended action

Find the file on the server and find out if it is accessible from external. If it is needed by the underlying software and contains critical data, you may can modify the access permissions (.htaccess, Linux permissions, ACL, ...). If it is not needed there, move or delete it.

It may be an automated backup of something by a plugin or other software. Try to configure it to store the backup in a place that is not accessible by anyone.

Revision #1
Created 4 August 2021 09:10:51 by Patrick Wall
Updated 4 August 2021 11:53:41 by Patrick Wall