Understand Nimbusec Results And Alerts
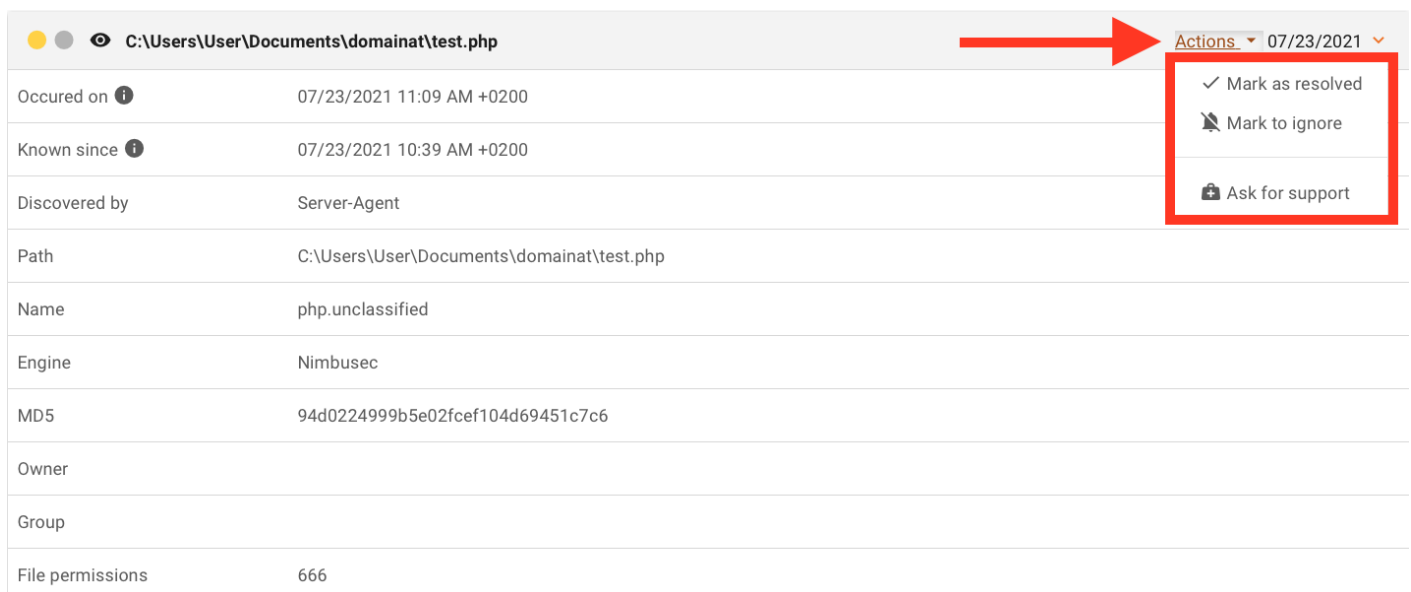
- Alert actions
- Blacklist alerts
- Content alerts
- Fading out results
- Server side alerts
- Reputation Alerts
- Issue and Event overview

Alert actions

Each alert offers the user the ability to perform three different actions:

- Mark as resolved
- Mark to ignore
- Ask for support

To trigger one of those actions, click on "Actions" on the top right corner of the relevant issue.

Mark as resolved

When an alert is "*marked as resolved*", the alert is hidden from the domain details view. If Nimbusec detects the same kind of alert again on your domain, it will generate a new alert and notification.

Use this action if you solved an issue and want to remove it from the list of alerts in Nimbusec.

The user has the possibility to add a comment to document this action.

Mark to ignore

When an alert is "*marked as ignored*", the alert is hidden from the domain details view. It also hides any alerts that are equivalent. If Nimbusec detects the same kind of alert again on your

domain, it will **not** generate any new alert or notifications.

Use this action if you or your security policy assigned a different risk level to a certain kind of alert that Nimbusec provides.

The user has the possibility to add a comment to document this action.

Ask for support

Use this option to contact the Nimbusec support team and get more information about this issue. The support team will help the user to understand and solve this problem.

Blacklist alerts

Blacklists are lists of internet addresses that are known for security problems. These lists are maintained by organisations like Google, cybersecurity companies or non-profits who try to warn about "black sheep" within the online community. There are two ways your website can end up on such a list:

- Your website poses a risk to its visitors. Nimbusec calls this a "blacklist result"
- Your website links to another website that poses a risk to its visitors. Nimbusec calls this a "suspicious link result".

Blacklist Result

Definition

The monitored domain has been found on a blacklist.

How is it detected

Nimbusec external scan checks a domain's reputation on multiple blacklists. If the domain shows up on a blacklist an alert is generated. Blacklist alerts always refer to the main domain Nimbusec is monitoring.

Alert levels

- *RED*: Domain is currently listed on a blacklist
- *YELLOW*: Domain is listed on a blacklist which gets its results from communities (e.g. Web of Trust)

Recommended action

Click "Additional Information" to access the blacklist's main portal to find out why your website has been listed. The blacklists description gives usually a good reason and at least is a starting point to fix the problem that led to blacklisting. Follow the individual blacklist's process to remove your domain from the list (rescan) and repair its online reputation.

Suspicious Link Result

Definition

The monitored domain includes external links that have been found on a blacklist.

How is it detected

Nimbusec Cloud Scan checks every external link's reputation on multiple blacklists. If an external linked domain shows up on a blacklist a "suspicious link" alert is generated.

Alert levels

- *YELLOW*: An external link shows up on a blacklist

Recommended action

Check directly on the blacklist's portal why the external link ("Reason") has been listed. Remove the link unless the external link is under your control. In this case, follow recommended actions of "Blacklist Alert".

Content alerts

Defacement

Websites are the most public representation of any modern enterprise. This combination of high publicity with complex technology makes websites a prime target for political hacktivists who aim to embarrass a company and cause as much damage as possible.

Website defacements therefore "consist of hacking into a web server and replacing a web page with a new page bearing some sort of message."
[Samuel, A. W. (2004). Hacktivism and the future of political participation, Harvard University, Cambridge, Massachusetts, p.8]

Technology-enabled political activism is often driven by major international and social disputes. These disputes are reflected in defacement waves that target a similar group of websites and communicate similar messages.

Examples for such "hacktivism" waves are:

- Anonymous with changing targets since 2003
- Syrian Electronic Army with pro-Assad messages aimed at new outlets, universities
- ISIS mass defacements in 2015

Our goal is zero false positives. Because of the advanced methods used here, we cannot guarantee 100% detection of a defacement, but we see the changes and tell if they are really suspicious.

Definition

A Nimbusec defacement alarm is defined by the following conditions:

- The visual appearance of a website was changed to distribute social, political or just for fun messages to the visitor.
- The website was changed in a way that the visitor will easily distinguish it from an official change. As a result, the main context of the website was replaced.
- The definition of a defacement is way to unspecific. @Nimbusec, **we also differentiate between a phishing attempt (placing links on the website) and a defacement like defined above**. You can find phishing attempts by the suspicious link alarm event (see blacklist category)

How is it detected

Nimbusec detects defacements typically from external, by its Cloud Scan.

Basically this is a fast approach that may detect defacements by signatures. Therefore the content of a website is extracted (plain text without tags and attributes). This content is then matched against an increasing set of rules which represent the content of typically seen defacements. Included are also bad words in multiple variations e.g. hacked by | h4cked | h4ck3d!!! | ...

To sum it up:

- Content is matched on rules, representing typical defacements
- Bad words are looked up in the content

We also gather data from external threat intelligence services. Defacement alarms are directly created from those data sources and are also used to write new signatures to improve the overall detection rate.

Alert levels

- *RED*: Identification of known defacement based on defacement signature.
- *YELLOW*: Possible defacement warnings detected by our external threat intelligence services that are not confirmed yet.

Red Alert

On red alerts a defacement was seen based on signatures. This can be held as defacements similar to the detection rate of anti virus products and should be taken really seriously. Automated reaction can be considered.

Yellow Alert

These alerts have to be taken serious as well, but we recommend to have a look at the page and verify the issue yourself.

Recommended action

The defacement result detail gives you a lot of information and has in mind to give you on first sight what went wrong.

Also screenshots of the landing page are rendered to see what our crawlers saw at the time of the scan.

The content result gives you the following information:

- Occured on: the time of the detection
- Reason: Description of the modules which voted for this issue
- Region: the region where the scan was performed from
- Viewport: a mobile or desktop browser client setting can be used
- Path: URL to the page/resource where the change was seen
- Change: Usually for this issue --> Defacement detected
- Name: Name of the defacement, if we have one (e.g. Hacker group). So you can identify the defacement better.

Try to verify the result by browsing the path, shown in the result. Request the website directly and also over a search engine. You may get different results. **Do this only from a secure environment, as defaced websites are also likely to spread malware!**

In case the website got defaced, and you don't have a incident response chain yourself, we prepared a short guide here.

1. It is always good to create a backup of the webspace before changing anything.
2. Redirect to a maintainance page, or in worst case to just a blank page, to not bring site visitors to danger.
3. Investigate to find the weak spot (Outdated CMS or other application, some plugin, ..)
4. Fix the vulnerabilities and remove evidence

The detected change might have been part of a major, but intentional content change. Contact the website's administrator for information.

When to mark as False Positive

If no problem shows and you are certain that no defacement took place, mark the alert as "false positive". This will create a rule that should prevent such alerts in the future. But every content is different and therefore hard to compare and analyse - If you have a specific alert that shows up unless you marked it as false positive, please contact us and we will work out a solution.

If you need in depth information about why this alert was generated, please contact nimbusec support.

Fading out results

An issue will be faded out when it is not seen again in between 2 weeks. This keeps your domain dashboard clean.

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.

Reputation Alerts

Suspicious Redirects

What is it?

A suspicious redirect is a redirect that has changed. Redirects are tracked with each scan, and if the redirect chain changes e.g. to a malicious website, or doesn't match the expected pattern a warning for suspicious behavior is thrown.

Where is it detected?

- Website Security Monitor

Alert Levels

- YELLOW: redirects may not be triggered on any visit, they might also be set on purpose by the web administrator.

Recommended Action

Check if the redirect is leading to the correct target. If the target is known as malicious, remove the redirect if possible immediately.

DNS Takeover

What is it?

A potential DNS takeover vulnerability was found. This means that an attacker may take control of a DNS server for resolving your hostname. The attacker can change the DNS record(s) to a server that he/she owns.
This issue type results from a misconfigured server. Domain's DNS records are controlled by DNS servers that anyone can use, but no one within this service claims the domain.

To perform a takeover, the name server has to be one of the currently known vulnerable DNS services that can be found here:

https://github.com/indianajson/can-i-take-over-dns?ref=blog.projectdiscovery.io

Where is it detected?

- Website Security Monitor

Alert Levels

- YELLOW: A potential DNS takeover vulnerability was found in the DNS configuration of your scanned website.

Recommended Action

- Delete the authoritative nameserver assigned to the domain
- (Re-)Activate the unused website (nameserver entry)

For more information, please check the following article:

https://blog.projectdiscovery.io/guide-to-dns-takeovers/

Issue and Event overview

Nimbusec Website Security Monitor

Issue Types 2022

Category	Issue Types	Descritpion
Malware	Malware	Malicious code fragments are found on a Web page. Typical examples would be, amongst others, credit card skimmers, crypto miners or tech scams.
	SEO-Spam	If changes on a website are detected while acting as 'googlebot' instead of the default browser agent a warning for suspicious behavior is thrown
Defacement	Defacement	The visual appearance of a website was changed to distribute social, political or just for fun messages to the visitor
	Content Violation	Changes of the content of a Web page are detected. These change may be intended by the website owner or may be the result of a malicious attack. However, Nimbusec does not distinguish between legitimate and malicious changes.
Reputation	Blacklist	The domain which is subject to review is found on blacklists monitored by Nimbusec
	Suspicious Link	Suspicious resources, based on blacklists monitored by Nimbusec, are embedded (but not loaded) on a Web page. A typical example of this type of event would be a link (a-tag) which points to a suspicious domain found in the Nimbusec blacklist.

	Suspicious Request	A suspicious resource, based on blacklists monitored by Nimbusec, is actively loaded by a Web page. A typical example of this type of event would be a JavaScript source which points to a suspicions domain.
Webshell	Webshell	Malicious code fragments are found in files monitored by Nimbusec's Server Agent. As files are directly inspected on the Web server additional malicious code such as Webshells may be detected.
Application	Vulnerable	An application with a possible vulnerability has been found on a website
	CMS Tampered	Core file of WordPress change and are only generated by Nimbusec's server agent. However, Nimbusec cannot not distinguish between legitimate and malicious changes.
	Outdated	An outdated application has been found on a website
TLS	TLS Expires	The TLS certificate will expire soon
	TLS Notrust	Untrusted root certificate
	TLS Protocol	Unsafe TLS protocol allowed in configuration
	TLS Sigalg	Bad signature algorithm
	TLS Ciphersuite	Unsafe TLS cipher allowed in configuration
	TLS Hostname	Hostname does not match certificate
	TLS Legacy	Symantec legacy certificate in use
	TLS Misconfigured Chain	The received certificate chain was incomplete or misconfigured
	TLS No Https redirect	HTTP website does not redirect to HTTPS
	TLS Revoked Cert	The certificate was revoked by the owner
Configuration	Baseline Empty	Wrong Agent configuration: empty result