BITNINJA SECURITY

monarx

BITNINJA - MONARX

MALWARE SCANNER COMPARISON

Malware continues to be a major threat to businesses, with new strains and variants constantly emerging. In order to protect against these attacks, it is essential to use a reliable and effective malware scanner. BitNinja and Monarx are two popular malware scanners that have recently been compared in a thorough testing process. The test was designed to focus on Javascript and PHP-based malicious files, as these are the most common types of malware.

THE TESTING METHOD:

The testing process was thorough and methodical. Three identical machines were used in the test, every machine ran with the latest available software versions, and the test was re-run three times to eliminate any errors.

The three machines used in the test had the following specifications:

vCPUs: 2 vCPUs - AMD Epyc-Rome
RAM: 4096 MB
Storage: 100 GB NVMe
OS: CentOS Linux release 7.9.2009

Benign files tested: 54792
Malicious files tested: 82846
Filetypes based on extension:
JavaScript: 36612
PHP: 17271
TXT: 838
Others: 28125

THE ONLY BARRIER

Unfortunately, Monarx was quite cautious and distrustful during the testing process, which resulted in a barrier for BitNinja. Monarx did not allow BitNinja to purchase their software or run more than one scan, so on some charts, estimated results are visible due to this limitation. Furthermore, during their trial, Monarx only allowed marking of malicious files, but not quarantining or cleaning. Consequently, BitNinja has stated that all data points that were collected on Monarx's own reporting may not accurately represent the capabilities of their software. This meant that BitNinja was not able to test Monarx equally, as Monarx preferred to hinder the testing process.

SCAN TIMES AND LOAD AVERAGES

During the tests, both BitNinja and Monarx **faced a mix of 137,680 malicious and benign files**. It took BitNinja's first "quick" scan around 6 minutes to complete, and the "deep" scan took 92 minutes. Monarx's scan time took approximately 5-6 minutes, but it is worth noting that this is only the scan time for Monarx and does not include cleaning and quarantining, which are performed by BitNinja during its scan time. Additional info to add here is that **Monarx's search engine** works with SHA256 hashes, which means that it may **take several hours for it to recognize and react to newly modified versions of malware.** This can potentially impact the effectiveness of the scanner in real-time situations.

Testing for **load resulted in an average of 0,55 for BitNinja and 0,4 for Monarx**. Although keep in mind that these result shows only in the scanning phase of Monarx and do not include cleaning, while **BitNinja simultaneously quarantines or cleans the files** with almost the same generated load. In fact, BitNinja has plans to further reduce the load on the system by **implementing a cloud scanner method in the first quarter of 2023.**

CLEANING AND QUARANTINING PERFORMANCE

It is important to note that the test servers were in a controlled environment and may not be perfectly representative of real-world results. However, BitNinja still stands behind the validity of the testing method and results. The dataset used in the test contained several different types of malware "unknown" to the engines, and was gathered from a variety of sources including the internet and internal test machines used as honeypots.
The focus of the test was on Javascript and PHP-based malicious files, as these are the two major players in the malware industry.

Firstly, the focus was on PHP. In this category, **BitNinja came out on top with an overall 8.4% over Monarx**. This was thanks to BitNinja's PHP Behaviour Analyzer combined with the Defense Robot, which generated more signatures.

Moving onto **Javascript-based malware, BitNinja caught an average of 25,000 files, while Monarx caught 36,612**. Although when **considering all file types, BitNinja came out on top with an average of 69,899** files caught or cleaned. **Monarx narrowly missed the mark with 64,143** files caught**.** Again, it is crucial to keep in mind, that the results of BitNinja were measured with their script based on file extension, while the numbers from Monarx are from their own dashboard, therefore it is not clear what these are based on.

FALSE POSITIVES

All malware scanner users' worst nightmare is generating false positives, which can bring down a website or cause user frustration. In this test, **Monarx had a false positive rate of 0.13%, catching 72 benign files as "malicious." BitNinja,** on the other hand**, had no false positives.**

While a false positive rate of 0.13% may not seem high, it can have significant consequences on a larger scale. For example, on a small to medium-sized hosting server with 5-10 million files, this rate could result in false positives for 6,500 to 13,000 files. This can cause frustration for users.

SUMMARY

Overall, both BitNinja and Monarx are strong performers in the field of malware scanning and protection. Although, there are some key differences between the two. One of the main differences is in the types of threats that each scanner is able to detect. BitNinja is designed to detect and block a wide range of threats, including malware, vulnerabilities, SQL injections, etc., while Monarx is primarily focused on detecting and blocking only malware. This means that BitNinja may be a better choice for businesses that are looking for a more comprehensive protection solution.

In conclusion, while BitNinja offers slightly more comprehensive protection and is able to detect and block a wider range of threats, Monarx is also an effective option for those looking to protect against malware attacks.

MEASUREMENTS	BITNINJA	MONARX
Detection Accuracy	82.68%	77.42%
False positives	0%	0.13%
Scan time*	5 min	5 min
Reaction time	1 sec	1 hour+
Server load	0,55	0,4

*First phase scan time

In case the complete data set is needed, it can be provided upon request!