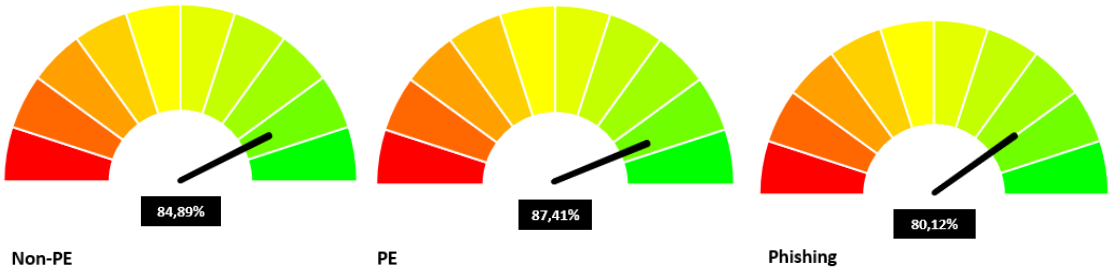
Evaluation of Vercara UltraDDR (UltraDNS Detection and Response)

A test commissioned by Vercara and performed by AV-TEST

Date of the test report: April 12, 2023 (version 1.00)

Executive Summary

In February 2023, AV-TEST performed a test of the Vercara UltraDDR, focusing on blocking malicious URLs and phishing websites as well as false positive avoidance. The test is evaluating the protection at 'time zero' as well as on differences in the detection found four hours later.



In order to ensure a fair review, Vercara did not supply any samples (such as malicious or clean samples, URLs or associated metadata) and did not influence or have any prior knowledge of the samples tested or the testing methodology. All links and malicious samples tested were verified by AV-TEST as recent and active.

The test focused on the detection rate of links pointing directly to portable executables (PEs) malware (e.g., EXE files), links pointing to other forms of malicious files (e.g., html, JavaScript) as well as phishing URLs. A total of 3,224 malicious samples were tested in the first run. After filtering out the CDNs/FH and reducing the sample set to unique domains the remaining samples consist of 735 phishing URLs, 441 PE malware URLs and 804 non-PE malware URLs.

Besides this, we evaluated the false positive rates using downloads for well-known applications from http and https websites. An additional false positive test was performed against known clean popular websites from Alexa's top list. A total of 2,523 test cases were used.

The full details of the test setup and the testing scenarios can be found in the following sections of this test report.

Test Overview

Every second, AV-TEST discovers three to four new malware variants. This sums up to around 9 million new malware every month, or more than 1.35 billion malware objects in total which are included in AV-TEST's database.

While most malware targets the Windows platform, protection for all operating systems is a required practice. Attaining protection against the growing number of threats is essential for all enterprises. Phishing is a great example of an attack that impacts all operating systems and relies on fooling the end user into thinking the site is legitimate so the attacker can steal sensitive information.

Vercara has commissioned AV-TEST to review their Vercara UltraDDR (UltraDNS Detection and Response).

Overview of Vercara UltraDDR

Vercara's UltraDDR (DNS Detection and Response), launched in partnership with HYAS Infosec, is a recursive DNS-based protection service that safeguards user internet traffic and enforces enterprise acceptable use policies. UltraDDR provides a Protective DNS solution that enables enterprises to get in front of threats by blocking communication before damage can occur. Protective DNS analyzes DNS queries and takes action to block outbound queries to malicious domains to mitigate threats before they take effect. Using years of historical domain data, UltraDDR delivers real-time observability of outbound network communication, allowing enterprises to detect and stop malware, ransomware, phishing, and supply chain attacks before they can do damage.

The service also boasts comprehensive DNS firewall capabilities that allow administrators to choose categories of internet traffic – such as adult, gambling, gaming, social media and more – that are deemed risky or not acceptable under company policy, and block or flag this traffic to provide a simple, unobtrusive way of enforcing policy.

Test Cases

All of the tests were performed in AV-TEST's laboratory in Magdeburg, Germany. All data used for testing, including all samples URLs and metadata, was exclusively sourced by AV-TEST.

Vercara did not have access to sample URLs before the testing, nor did it provide such data for the testing. All samples were previously verified by AV-TEST as known to be malicious. We use static and dynamic analysis of samples to ensure that the domains are actively hosting malicious content at the time of the testing and exhibiting their malicious behavior.

Both performed tests were split into three categories, covering the different types of attacks:

- URLs pointing to malicious PE files (for Windows, EXE files)
- URLs with other malicious destinations (non-PE files, usually html or php websites, including links to scripts such as JavaScript or VBS)
- Links to phishing websites

A total of 3,224 samples were used for the initial test-run ('time zero'). This included 788 malicious links to PE files, 1385 links to other files with other malicious content (non-PE), and 1,051 samples of phishing websites. For the retest after 4 hours, some URLs didn't work anymore, as they were taken offline (e.g., by the attacker or internet provider). Therefore, only 3,093 test cases were used, including 742 links to PE files, 1374 links to non-PE files and 977 phishing URLs.

DNS protection solutions are designed to protect networks by blocking or redirecting requests to malicious domains, based on DNS query data. These solutions operate at the DNS layer, intercepting and filtering DNS requests and responses.

However, DNS protection solutions do not inspect the actual traffic flowing between the client and the server. This is because the DNS protocol operates at a different layer of the network stack than the application layer protocols that are used to deliver web content, such as HTTP or HTTPS.

That's why we filtered out CDNs/FH and reduced the sample to unique domains. The remaining samples were in the initial test 441 PE URLs, 804 Non-PE URLs, 735 Phishing URLs and 429 PE URLs, 794 Non-PE URLs, 674 Phishing URLs in the retest after 4 hours.

For false positive testing, AV-TEST used the following types of known clean files and websites from http and https sources:

- URLs pointing to clean file downloads (mainly PE for Windows, EXE files)
- URLs with other non-malicious destinations (non-PE files, usually clean html or php websites)

All samples used for the false positive testing were carefully selected and validated. In an exhaustive review by AV-TEST, the samples did not show any signs of malicious behavior and were considered clean. A total of 2,523 clean websites and downloads were used for the initial test (1,050 downloads and 1,473 websites). For the test-run 4 hours later, a total of 2514 samples could be used (1,045 downloads and 1,469 websites).

All URLs were accessed on virtualized Windows systems running Windows 10 Professional (English, 64 bit), with all patches installed.

All download attempts were triggered using Python scripts to access the URLs for the test. Testing included checking if access to the URL was successful or if it was blocked by the product. The tests were performed during the period of February 2 to 23, 2023.

CDNs and File Hosting Services

CDNs (Content Delivery Networks) and FH (File Hosting) services are used by websites and applications to deliver their content more quickly and reliably. These services provide a distributed network of servers that cache and deliver content to users from the nearest server location, reducing latency and improving performance.

When a DNS protection product blocks a CDN or FH service, it prevents users from accessing the content served by that service. This can have several negative consequences:

1. Reduced website/app performance: Without access to the CDN/FH service, users may experience slower load times or disruptions in service, which can lead to a poor user experience.

2. Increased server load: If the CDN/FH service is blocked, requests for content will be directed to the origin server instead, which can increase the load on the server and potentially cause it to become overwhelmed and fail.
3. Inability to access legitimate content: Many legitimate websites and applications use CDNs/FH services, so blocking these services can prevent users from accessing content that they legitimately need.
4. Increased security risk: By blocking CDNs/FH services, DNS protection products may inadvertently allow users to bypass security measures put in place by the CDN/FH service, increasing the risk of cyber attacks and data breaches.

Overall, it's generally a bad idea to block CDNs/FH services in DNS protection products, as it can negatively impact website/app performance, increase server load, prevent access to legitimate content, and increase security risks. Instead, DNS protection products should be configured to allow access to legitimate CDNs/FH services while blocking malicious ones.

Test Results

For PE file URLs, Vercara initially scored 87.30% and increased to 87.41% in the retest as its top efficacy test category. Nearly as effective, Non-PE file URLs initially scored 84.70% and increased to 84.89% in the retest. Detection of phishing URLs showed a improvement from the initial score of 78.78% by increasing to 80.12% in the retest. False positives were low in the initial test at 2.54% and stayed at 2.55% in the retest to remain a low risk.

The detailed results of the detection tests are as follows (higher is better):

	Initial 'time zero' test			Retest after 4 hours		
Detection Rate	Reference	Detected	In percent	Reference	Detected	In percent
… of PE malware	441	385	87.30%	429	375	87.41%
… of Non-PE malware	804	681	84.70%	794	674	84.89%
… of phishing URLs	735	579	78,78%	674	540	80.12%

The retest after 4 hours showed improvements in detection rates for all three areas with notable improvement in the phishing URL detection rate.

For the false positive testing, the detailed results are the following ones (lower is better):

	Initial 'time zero' test			Retest after 4 hours		
False Positive Rate	Reference	Detected	In percent	Reference	Detected	In percent
… of good applications	1,050	41	3.90%	1,045	41	3.92%
… of popular Alexa URLs	1,473	23	1.56%	1,469	23	1.57%

As one can see, the false positive rate increased slightly in the second run due to the smaller number of tested URLs. The same number of false positives were seen on each run and the risk of a false positive remains on a low level. According to Vercara, any desirable URLs that are blocked by UltraDDR may be explicitly allowed via a configuration change.

Conclusion

Vercara UltraDDR was tested independently by AV-TEST with no knowledge of samples tested, testing methodology, or providing samples for the testing. Threat efficacy detection results peaked to 87.41% for PE file URLs in the retest and false positives remained a low risk for initial and retesting.