OpenDNS

Take Your Security Further™

An Introduction to Third-Party Reports from OpenDNS's CTO

We often are asked, *"How effective is OpenDNS Umbrella at blocking threats?"*
Or even, *"How does it compare to other solutions?"*

As we have highlighted, testing the efficacy of a security solution is a complex challenge. In order to ensure real-world results, we believe that you should evaluate our solution and others in your own production environment or an environment that provides a reasonable simulation. When you test in your own environment it is possible to compare the results of the test with your established security baseline to measure the actual impact on your organization. This is why we offer a two-week free trial.

Our customers overwhelmingly agree that real-world testing is the best way to prove the efficacy of any solution. That said, not all customers have the luxury of running a test in their real-world environment and they ask for third party validation. Third party validation can be provided by a current customer that uses the product and we encourage all prospective users to reach out to their peer group for references. Third party validation can also be provided by a testing facility.

The challenge with any third-party is that they use a different environment than yours. They test different threats than the ones you might encounter tomorrow. With different test environments for each evaluation it is easy for three different security providers to each sponsor a separate report that says their product is superior to the others. While we're not saying that one product cannot be better than others, such reports are not likely to prove it.

However, many people still ask for third-party validation of our product. So we commissioned AV-TEST, a long-established and reputable third-party, to evaluate Umbrella. Our instructions were straight forward—start a two-week trial as our customers would, then test whether or not we block domains that host malware or botnet C&C servers that are used to compromise systems and exfiltrate data. We were excited by the results, and we think you will be too.

We know it's just one data point in a market of over-hyped claims. Transparency is one of the OpenDNS Security Labs' key virtues, so please tell us how we can help you get more data to make the best decision.

Thank you for checking out OpenDNS.

Sincerely,

Dan Hubbard
OpenDNS CTO

135 Bluxome St. San Francisco, CA 94107

p + 1-415-344-3200 | **s** +1-877-811-2367

www.opendns.com

Blocking malicious hosts and C&C traffic with OpenDNS Umbrella

A test commissioned by OpenDNS and performed by AV-TEST GmbH

Date of the initial report: 29nd April 2015. Last update: 4th May 2015

Executive Summary

In April 2015, AV-TEST reviewed the cloud-delivered network security service OpenDNS Umbrella. OpenDNS offers its service as an additional protection layer to classic web gateway solutions or endpoint security products. Blocking malicious hosts via DNS means that access is blocked at the earliest stage with minimal performance impact. With its unique approach OpenDNS is not only able to prevent infections but also prevent data exfiltration to command and control (C&C) destinations if systems have already been compromised.

AV-TEST determined OpenDNS Umbrella has a blocking rate of 97.7% for malicious hosts.

Test Setup and Methodology

OpenDNS Umbrella has an online web-interface to configure policies and view reports and statistics. To enforce policies on a computer, the administrator has three options. (1) Use an existing network egress to point DNS traffic to OpenDNS; (2) Deploy the OpenDNS Virtual Appliance within a network to forward DNS traffic to OpenDNS; or (3) install the OpenDNS Roaming Client on the computer to forward DNS traffic to OpenDNS.

To setup the tests, AV-TEST installed the OpenDNS Roaming Client on a Windows 7 Virtual Machine. This Roaming Client is a lightweight component that configures the computer's DNS settings. The setup procedure was straightforward and completed within one minute without a reboot.

During the test, the computer resolved several thousand host names that were discovered to host malicious payloads and C&C servers. In case of a prohibited host the OpenDNS service responded with a special IP address that pointed to a Web server hosting a block page. If the host was not blocked by OpenDNS, the DNS response included the original IP address for the host. The host names were gathered by AV-TESTs own malware analysis systems during dynamic malware analysis and sharing with independent third parties. To ensure that infections or data exfiltration would be stopped in time, the offset between the appearance of a malicious host name in AV-TESTs analysis systems and testing that the OpenDNS service blocked the host was less than 5 minutes.

Test Results

Tested hosts are split into two categories. The first category contains hosts which are known to host active C&C servers and thus control zombies of a botnet. The second category contains other malicious hosts, which are known to serve current malicious payloads – including zero-days – or phishing pages.

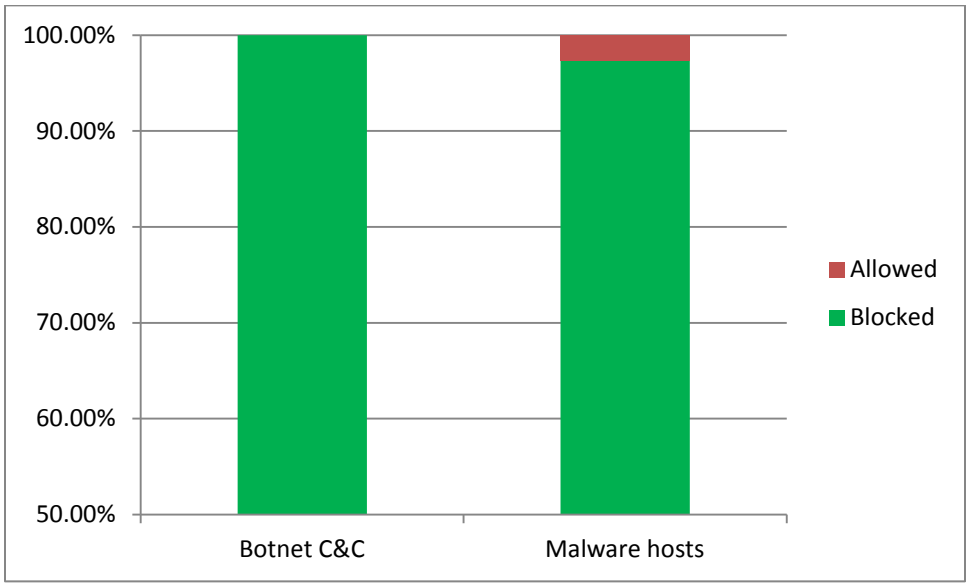

Figure 1: Blocking of malicious hosts

OpenDNS was able to classify & block 100% of the tested 338 C&C servers.

In the second category 97.31% of the 1895 hosts were blocked. There might be legitimate reasons to allow certain hosts on the DNS level in this category. If a malicious payload is hosted on code.google.com[1] (e.g. code.google.com/evil.exe), this domain shouldn't be blocked by DNS as the majority of hosted content on this domain is legitimate and not malicious (e.g. code.google.com/good.exe). OpenDNS uses a proxy-based security layer they call "Intelligent Proxy" for a limited number of hosts, but for the tested hosts, none were proxied.

The combined blocking rate of both categories was 97.72%.

To verify the efficacy of OpenDNS' domain classification Umbrella was also tested against 2,000 legitimate domains in a false positive test. OpenDNS misclassified a single domain only, which equates to a false positive rate of 0.05%.

[1] code.google.com was only mentioned as an example here, as it was known to host malicious content in the past http://www.v3.co.uk/v3-uk/news/2289683/google-code-fast-becoming-hackers-malware-mule

Conclusion

OpenDNS Umbrella has proven its abilities to block malicious hosts with a rate of 97.72%, while it has only a false positive rate of 0.05%. Due to its unique approach to protect the endpoint on the DNS level it has also no additional performance impact. OpenDNS hosts its multi-tenant service in 25 data centers all over the world. There is no additional overhead by a DNS request to OpenDNS compared to a DNS request to any other DNS server. The easy deployment and policy administration in their cloud-based web-interface is another positive point.

About the AV-TEST Institute

AV-TEST GmbH is an independent supplier of services in the fields of IT Security and Antivirus Research, focusing on the detection and analysis of the latest malicious software and its use in comprehensive comparative testing of security products.

Due to the timeliness of the testing data, malware can instantly be analyzed and categorized, trends within virus development can be detected early, and IT-security solutions can be tested and certified. The AV-TEST Institute's results provide an exclusive basis of information helping vendors to optimize their products, special interest magazines to publish research data, and end users to make good product choices.

AV-TEST has operated out of Magdeburg (Germany) since 2004 and employs more than 30 team members, professionals with extensive practical experience. The AV-TEST laboratories include 300 client and server systems, where more than 1,000 terabyte of independently-collected test data, containing both malicious and harmless sample information, are stored and processed.

Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web http://www.av-test.org