Malicious Domain Blocking and Reporting (MDBR)

Setup Instructions

Congratulations on signing up for our Malicious Domain Blocking and Reporting (MDBR) service! The final step to complete your enrollment for the service is to configure your local forwarder to send DNS queries to Akamai's primary and secondary recursive DNS servers at 96.7.136.4 and 96.7.137.4.

Typically, you can configure these "forwarders" in the same location where you manage other settings for your DNS. The following are the most common scenarios, but will be dependent on your organization's specific DNS setup:

For Windows Servers:

DNS settings management is available as an Administrative Tool in the Control Panel. Once you access the DNS management tool, edit the Forwarders, which are located in Properties, to include the IP addresses for Akamai's primary and secondary recursive DNS servers (96.7.136.4 and 96.7.137.4).

For organizations using BIND:

Open and modify the named.conf.options file to include the IP addresses for Akamai's primary and secondary recursive DNS servers (96.7.136.4 and 96.7.137.4) in the Forwarders area.

For organizations using a Next-Generation Firewall (NGFW) or Secure Web Gateway (SWG) product:

Navigate to the DNS Proxy or Server settings for your organization's applicable product, and enter the IP addresses for Akamai's primary and secondary recursive DNS servers (96.7.136.4 and 96.7.137.4).

To test your organization's DNS change:

After configuring your local forwarder to send DNS inquiries to Akamai's recursive servers, you can test that your DNS change was successful with the following URLs:

- CnC: akamaietpcnctest.com
- Phishing: akamaietpphishingtest.com
- Malware: akamaietpmalwaretest.com

If the service is operating properly, you will be directed to a pre-configured block page, indicating that access to the website it prohibited. If your organization's DNS requests are not reaching Akamai's servers, you will be directed to a demonstration website indicating that Akamai Enterprise Threat Protector (ETP) has not been set up correctly.

For step-by-step guides on how to configure DNS forwarding, please visit Akamai's Enterprise Threat Protector Help website.

For additional information and troubleshooting, please visit the CIS MDBR FAQ page.

For questions or additional help in setting up DNS forwarding, please contact soc@cisecurity.org.

Additional DNS Configuration Guidance

False Positives Regarding Network Security Devices

In some situations, network perimeter security devices, such as firewalls and web proxies, have been found to make large amounts of outbound DNS requests for malicious domains which do not originate from compromised systems. This activity creates false positive alerts due to those devices proactively making DNS requests related to malicious domains on the device's block list. This also will skew MDBR reporting back to the affected entity due to the artificially high number of blocked DNS requests.

If your perimeter devices have the capability to proactively update malicious block lists, it is recommended that DNS requests originating from those specific devices be directed to another DNS provider and not be sent to Akamai.

Utilizing multiple recursive DNS servers

Utilizing the MDBR service requires configuring your organization's DNS infrastructure to use Akamai's recursive servers as its primary and secondary DNS forwarders. When reconfiguring your DNS infrastructure, you have two options:

1. Setting DNS forwarders to point to Akamai's primary and secondary forwarders only.
2. Setting DNS forwarders to point to Akamai's primary and secondary forwarders, in addition to setting tertiary and quaternary options that utilize a separate DNS provider or providers.

With option one, all DNS requests are sent to Akamai for review and logging. If a given request is determined to be malicious, it will be blocked, logged, and can be reported on. Directing all DNS requests exclusively to Akamai allows for consistent blocking of malicious activity, as well as more complete reporting, as the entirety of your organization's DNS queries can be accounted for.

However, relying on a single vendor's DNS service can introduce a single point of failure if the vendor were to experience an outage. In the unlikely event of a DNS provider outage, your organization would not be able to resolve DNS queries, which severely limits your network's ability to access the internet. In this scenario, the fix would be to make an immediate configuration change to direct outbound DNS queries to another DNS provider.

For step-by-step guides on how to configure DNS forwarding, please visit Akamai's Enterprise Threat Protector Help website.

For additional information and troubleshooting, please visit the CIS MDBR FAQ page.

For questions or additional help in setting up DNS forwarding, please contact soc@cisecurity.org.

Implementing option two helps alleviate the possibility of experiencing an internet outage, as it adds fault tolerance to your organization's DNS infrastructure. Adding multiple DNS forwarders, from different providers, allows DNS names to continue to be resolved in the event of a DNS provider outage.

However, the drawback to adding additional DNS forwarders is reduced visibility with MDBR, which would result in incomplete reporting should any non-Akamai DNS servers be utilized to resolve domain names. Additionally, if non-security-focused DNS providers are chosen as tertiary or quaternary options, the potential exists for malicious domains to be resolved. If your organization chooses to add additional DNS forwarders to your internal forwarder list, CIS recommends adding additional security-focused DNS service providers such as Quad9 (9.9.9.9) and Cisco's Umbrella service (208.67.222.222 & 208.67.220.220) as third and fourth options.

Please reach out to soc@cisecurity.org for more information or if you have any questions.

For step-by-step guides on how to configure DNS forwarding, please visit Akamai's Enterprise Threat Protector Help website.

For additional information and troubleshooting, please visit the CIS MDBR FAQ page.

For questions or additional help in setting up DNS forwarding, please contact soc@cisecurity.org.