

Microsoft released Sysmon 10 with DNS query logging feature

Microsoft has released the Sysmon 10 tool today and comes with the long-awaited DNS query (DNS Query Logging) feature.

Microsoft has released the Sysmon 10 tool today and comes with the long-awaited DNS query (DNS Query Logging) feature. Accordingly, this feature will allow Sysmon users to log DNS queries performed on the monitored computer, and this will also include query execution.

If you don't already know, Sysmon (aka) System Monitor is a Sysinternals tool that allows users to monitor certain activities on the computer and write information about those activities to the Windows Event Viewer.

1. It is possible to download official ISO files for Windows 10 20H1

To download Sysmon 10 to your computer, you can visit the Sysinternals website or download it from <https://live.sysinternals.com/sysmon.exe>. After the software has been successfully downloaded, you need to run it in the advanced command prompt (command prompt with administrative rights), because this tool requires administrator privileges to be able to launch.

```

Administrator: Command Prompt

System Monitor v10.0 - System activity monitor
Copyright (C) 2014-2019 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Usage:
Install: sysmon -i [<configfile>]
          [-h <{sha1|md5|sha256|imphash[*],...>] [-n <process,...>]
          [-l <process,...>]
Configure: sysmon -c [<configfile>]
           [--[-h <{sha1|md5|sha256|imphash[*],...>] [-n <process,...>]
           [-l <process,...>]]]
Uninstall: sysmon -u [force]

-c Update configuration of an installed Sysmon driver or dump the
  current configuration if no other argument is provided. Optionally
  take a configuration file.
-d Specify the name of the installed device driver image.
  Configuration entry: DriverName.
  The service image and service name will be the same
  name of the Sysmon.exe executable image.
-h Specify the hash algorithms used for image identification (default
  is SHA1). It supports multiple algorithms at the same time.
  Configuration entry: HashAlgorithms.
-i Install service and driver. Optionally take a configuration file.
-l Log loading of modules. Optionally take a list of processes to track.
-m Install the event manifest (done on service install as well).
-n Log network connections. Optionally take a list of processes to track.
-r Check for signature certificate revocation.
  Configuration entry: CheckRevocation.
-s Print configuration schema definition of the specified version.
  Specify 'all' to dump all schema versions (default is latest).
-u Uninstall service and driver. Adding force causes uninstall to proceed
  even when some components are not installed.

The service logs events immediately and the driver installs as a boot-start driver to capture activity from early in
  
```

Sysmon 10.0

1. Apple's new iCloud Windows 10 application is now available in MS Store

If running simply without any arguments, the program will display its usage information and for more details, you can visit Sysmon's Sysinternals website.

By default, Sysmon will monitor basic information such as creating processes and modifying file times. However, you can also configure this tool to monitor other events such as loading drivers, creating files, Registry events, and more.

There is a notable new point in Sysmon 10.0, which is that Microsoft has added the ability to monitor DNS queries and executable files that execute queries. This feature will need to be enabled via the configuration file with the DNSQuery directive.

An example of a very basic configuration file that allows DNS query logging is shown below. This configuration file can be installed with **sysmon.exe -i config.xml** in case sysmon is not installed, or **sysmon.exe -c config.xml**, in case sysmon is already running.

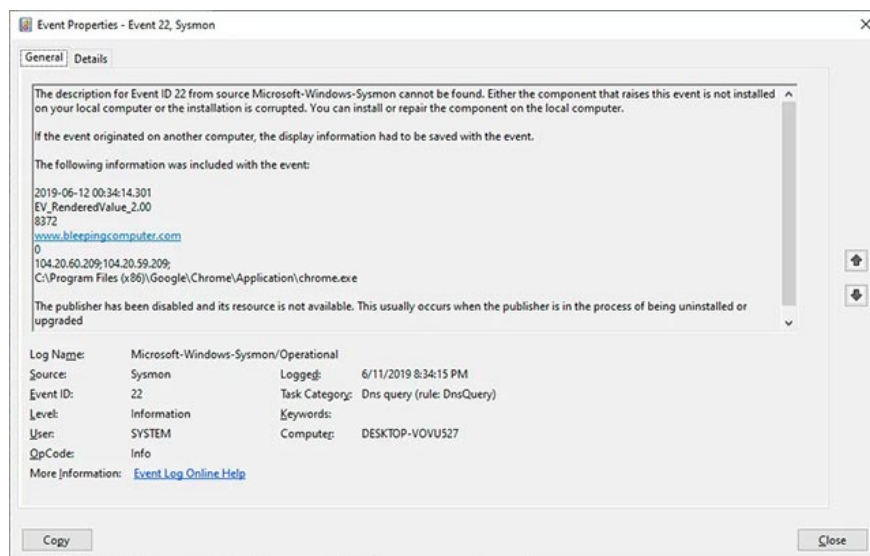
```
config.xml - Notepad
File Edit Format View Help
<Sysmon schemaversion="4.21">
  <EventFiltering>
    <DnsQuery onmatch="exclude"/>
  </EventFiltering>
</Sysmon>
```

Enable DNSQuery logging feature

1. The input experience in Windows 10 20H1 update will be significantly better, and this is the reason

When Sysmon is started with the above configuration file, it will start logging DNS query events (DNS Query) into the **Applications and Services Logs / Microsoft / Windows / Sysmon / Operational** section in **Event Viewer**.

Below you can see an example of Chrome querying DNS for the *www.bleepingcomputer.com* address when we visit this site.



Example of DNS query logging

1. Search and activate hidden features in Windows 10 with Mach2 tool

The example above is just a small sketch of the overall picture of what System Monitor can do. If you want to learn how to use this software, I really recommend reading the documentation on the Sysinternals page.

In case you only want to access and use the Sysmon configuration file available to detect malicious traffic and threats, you can use SwiftOnSecurity's Sysmon configuration file on GitHub.

You finished reading the article "**Microsoft released Sysmon 10 with DNS query logging feature**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.