

Forum:[Hack Forums](#)

Thread: [Detecting Enabled Anti-Virus | Windows COM | WMI Query | Python Source Code](#)

Hackers - May 4, 2024, 7:36 am

Hello, today I will be showing you a prototype script I wrote that can fetch the details about your computer's anti-virus.

This is good for making sure your software is up to date, and to verify that you are protected.

Interested in more of this content?

Thank [Fallen](#) members!

We are using Python today, with the win32com package to interact with lower level Windows functions.

```
Code import win32com.client
```

```
objWMIService = win32com.client.Dispatch("WbemScripting.SWbemLocator")
```

```
swbemServices = objWMIService.ConnectServer(".", "ROOT\\SecurityCenter2")
```

We use COM on Windows, in combo with the WMI service. This allows us to execute basic SQL queries to find more information.

```
Code SELECT * FROM AntivirusProduct
```

Once we get the results, we must loop through them to analyze.

We can get the display name, product state (enabled/disabled), and other information.

```
Code for objItem in collItems:
```

```
    name = objItem.displayName
```

```
    state = objItem.productState
```

```
    state_hex = f'{state:06x}' # Format as hex with leading zeros
```

The values are represented with hex values, which can obviously be interpreted in binary or other types too.

For hex, we can extract certain values to know if it is enabled or not.

For example, Windows defender may have a state of "060100". This is also represented as "0x60100"

You can get the "middle number", which would be "01" - as in there is "06 on the left" and "00 on the right"

- if this middle number = "10" then it is enabled, and if not, it is disabled.

- for Windows Defender in this case of 060100, the "01" means it is disabled.

When we look at my computer, AVG is set to "041000" or "0x41000". This is "04 on left" and "00 on right", which is "10" in the middle for enabled.

Code Antivirus Name: Windows Defender

State (Hex): 060100

Enabled Status: Disabled

Update Status: Up to Date

Antivirus Name: AVG Antivirus

State (Hex): 041000

Enabled Status: Enabled

Update Status: Up to Date

Lastly, we can use the last 2 numbers of the hex value to see if it's up to date or not.

If the last 2 digits are "00" this means it is updated already to latest available version, for your OS. For example "060100" ends in "00" and so does "041000" so we know that both AV options are updated on my current machine.

Full Source Code:

```
Code import win32com.client
```

```
def check_antivirus_status():
    # Connect to the WMI service
    objWMIService = win32com.client.Dispatch("WbemScripting.SWbemLocator")
    swbemServices = objWMIService.ConnectServer(".", "ROOT\\SecurityCenter2")

    # Execute the WMI query to get antivirus product information
    collItems = swbemServices.ExecQuery("SELECT * FROM AntivirusProduct")

    # Check the status of each antivirus product
    for objItem in collItems:
        name = objItem.displayName
        state = objItem.productState
        state_hex = f'{state:06x}' # Format as hex with leading zeros

        # Extract the middle two hex digits and check if enabled
        enabled_hex = state_hex[2:4]
        enabled_status = 'Enabled' if enabled_hex == '10' else 'Disabled'

        # Extract the last two hex digits for update status
        update_hex = state_hex[4:6]
        update_status = 'Up to Date' if update_hex == '00' else 'Not Up to Date'

        print(f'Antivirus Name: {name}')
        print(f'State (Hex): {state_hex.upper()}')
        print(f'Enabled Status: {enabled_status}')
        print(f'Update Status: {update_status}\n')

if __name__ == "__main__":
    check_antivirus_status()
```

Ya_Sanya__ - May 18, 2024, 12:53 pm

Thank you, is it working for all antiviruses?

Hackers - May 20, 2024, 4:56 am

(May 18, 2024 12:53 PM)Ya_Sanya__ Wrote: [CITE](#) Thank you, is it working for all antiviruses? It should be using the same formatting for statuses, so as long as it's either a minifilter or another registered product for Windows, it should show up with info.

7 - May 31, 2024, 6:42 am

Very nice.

This could also be very useful for adding the right exceptions to an AV once the correct AV is detected, could it not?

Hackers - May 31, 2024, 6:44 am

(May 31, 2024 06:42 AM)NulldB Wrote: [\[CITE\]](#) Very nice.

This could also be very useful for adding the right exceptions to an AV once the correct AV is detected, could it not?

Yep, exactly, if you need your personal programs to respond differently based on the AV / to support different types of features then you can do that.

obtainhigh - July 4, 2024, 3:06 am

needed some debugging to perfect it.

Working code:

PHP Code

```
<?php
import win32com.client

def get_wmi_service(namespace):
    """Connect to the WMI service."""
    locator = win32com.client.Dispatch("WbemScripting.SWbemLocator")
    return locator.ConnectServer(".", namespace)

def fetch_antivirus_info(wmi_service):
    """Fetch antivirus product information using WMI."""
    return wmi_service.ExecQuery("SELECT * FROM AntivirusProduct")

def parse_product_state(state):
    """Parse the product state to determine enabled and update status."""
    state_hex = f'{state:06x}'
    enabled_status = 'Enabled' if state_hex[2:4] == '10' else 'Disabled'
    update_status = 'Up to Date' if state_hex[4:6] == '00' else 'Not Up to Date'
    return state_hex.upper(), enabled_status, update_status

def display_antivirus_info(products):
    """Display the antivirus product information."""
    for product in products:
        name = product.displayName
        state_hex, enabled_status, update_status = parse_product_state(product.productState)
        print(f'Antivirus Name: {name}')
        print(f'State (Hex): {state_hex}')
        print(f'Enabled Status: {enabled_status}')
        print(f'Update Status: {update_status}\n')

def check_antivirus_status():
    """Main function to check the status of antivirus products."""
    wmi_service = get_wmi_service("ROOT\SecurityCenter2")
    products = fetch_antivirus_info(wmi_service)
    display_antivirus_info(products)

if __name__ == "__main__":
    check_antivirus_status()
```

riesax - July 23, 2024, 1:30 am

Thanks a lot. Learns a lot from these kind of things! Would love to be as good

Hackers - November 19, 2024, 12:39 pm

(Jul 4, 2024 03:06 AM)obtainhigh Wrote: [\[CITE\]](#) needed some debugging to perfect it.

Working code:

PHP Code

```
<?php
import win32com.client

def get_wmi_service(namespace):
    """Connect to the WMI service."""
    locator = win32com.client.Dispatch("WbemScripting.SWbemLocator")
    return locator.ConnectServer(".", namespace)

def fetch_antivirus_info(wmi_service):
    """Fetch antivirus product information using WMI."""
    return wmi_service.ExecQuery("SELECT * FROM AntivirusProduct")

def parse_product_state(state):
    """Parse the product state to determine enabled and update status."""
    state_hex = f'{state:06x}'
    enabled_status = 'Enabled' if state_hex[2:4] == '10' else 'Disabled'
    update_status = 'Up to Date' if state_hex[4:6] == '00' else 'Not Up to Date'
    return state_hex.upper(), enabled_status, update_status

def display_antivirus_info(products):
    """Display the antivirus product information."""
    for product in products:
        name = product.displayName
        state_hex, enabled_status, update_status = parse_product_state(product.productState)
        print(f'Antivirus Name: {name}')
        print(f'State (Hex): {state_hex}')
        print(f'Enabled Status: {enabled_status}')
        print(f'Update Status: {update_status}\n')

def check_antivirus_status():
    """Main function to check the status of antivirus products."""
    wmi_service = get_wmi_service("ROOT\\SecurityCenter2")
    products = fetch_antivirus_info(wmi_service)
    display_antivirus_info(products)

if __name__ == "__main__":
    check_antivirus_status()
```

Thanks, I really appreciate the effort!

(Jul 23, 2024 01:30 AM)riesax Wrote: [\[CITE\]](#) Thanks a lot. Learns a lot from these kind of things! Would love to be as good

I'm still learning myself!! How's it going on your side & do you have any questions?

Stanley - March 16, 2026, 8:31 pm

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

yigliman - *March 30, 2026, 9:15 am*

I'd like to know how to obfuscate my .exe file or how to make it undetectable by antivirus software.