

Forum:[Hack Forums](#)

Thread: [Easy Anti-Anubis aka Analyzing the Analyzer \[](#)

Raz?r - November 7, 2012, 4:40 pm

Hey guys,

today i show you how to make an Anti-Anubis function easy.
I never tried this before and am coding it live while writing this tut.
I will use it for RazorCrypt if it works, i think :P

I will explain it with AutoIT code as this is easy to understand.

So at first we need to find out a few information about their PCs.
I made a little AutoIT script for this.

```
Code MsgBox(0,"","@OSArch = "&@OSArch& "@OSBuild = "&@OSBuild& "@OSLang = "&@OSLang& "@OSServicePack = "& @OSServicePack& "@OSType = "& @OSType& "@OSVersion = "& @OSVersion& "@Computername = "& @ComputerName& "@UserName = "& @UserName)
```

This was the result:

[img]http://anubis.iseclab.org/?action=result_img&task_id=1a324c52d485a9174b9e60acd3ea64473&image=1.png[/img]

So we have the following information:

They use Windows XP SP 3
The username is Administrator
and the PC name is: pc + a number between 1 and 10

So let's start with a func we name "_couldbeanubis"

```
Code Func _couldbeanubis()  
    If StringInStr(@OSVersion,"XP") And StringInStr(@UserName,"Admin") And  
StringInStr(@ComputerName,"pc") And StringInStr(@OSServicePack,"3") Then  
        return True  
    Else  
        Return False  
    EndIf  
EndFunc
```

So let's run it on anubis to see if it returns "True".
I will use a MessageBox for this again.

So here is the result:

[img]http://anubis.iseclab.org/?action=result_img&task_id=183a7ecabe1b970f4094a4795ae8cee8d&image=1.png[/img]

ok so now this doesn't guarantee that this actually IS an anubis comp.

So let's get a few more details. I guess starting with getting all running processes should help.
So my friend AutoIT you need to help me again.

So let's use this simple piece of code:

```
Code #include <array.au3>
```

```
$list = ProcessList()
```

_ArrayDisplay(\$list)I will run this now twice to see if there are similar processes that aren't usual on WINXP pc's.

So here are the results.:

[img]http://anubis.iseclab.org/?action=result_img&task_id=180f95f925000b9f48191b868539a713f&image=1.png[/img][img]http://anubis.iseclab.org/?action=result_img&task_id=15564e4dd949fc2749da265efe5ed0021&image=1.png[/img]

We will target Row 18-21 as this processes are in the same order on every anubis scan!

So, this code should finally find out if we are on one of Anubis comps:

```
Code $list = ProcessList()
```

```
Func _isanubis()
```

```
If _couldbeanubis() = True Then
```

```
    If $list[18][0] = "msmsgs.exe" And $list[19][0] = "reader_sl.exe" And $list[20][0] = "alg.exe" And  
    $list[21][0] = "wscntfy.exe" Then
```

```
        return True
```

```
    Else
```

```
        Return False
```

```
    EndIf
```

```
Else
```

```
    return False
```

```
EndIf
```

```
EndFunc
```

```
Func _couldbeanubis()
```

```
    If StringInStr(@OSVersion,"XP") And StringInStr(@UserName,"Admin") And  
    StringInStr(@ComputerName,"pc") And StringInStr(@OSServicePack,"3") Then
```

```
        return True
```

```
    Else
```

```
        Return False
```

```
    EndIf
```

```
EndFunc
```

Now let's test it! I made an AutoIT executable for this again:

```
Code $list = ProcessList()
```

```
If _isanubis() = True Then
```

```
    MsgBox(0, "", "Sorry, but Anubis Scans can't help you this time")
```

```
    Exit
```

```
EndIf
```

```
MsgBox(0,"","test")
```

```
Func _isanubis()
```

```
If _couldbeanubis() = True Then
```

```
    If $list[18][0] = "msmsgs.exe" And $list[19][0] = "reader_sl.exe" And $list[20][0] = "alg.exe" And  
    $list[21][0] = "wscntfy.exe" Then
```

```
        return True
```

```
Else
    Return False
EndIf
```

```
Else
    return False
EndIf
```

```
EndFunc
```

```
Func _couldbeanubis()
    If StringInStr(@OSVersion,"XP") And StringInStr(@UserName,"Admin") And
StringInStr(@ComputerName,"pc") And StringInStr(@OSServicePack,"3") Then
        return True
    Else
        Return False
    EndIf
EndFunc
So this was the result:
```

[img]http://anubis.iseclab.org/?action=result_img&task_id=163e8fd95f278e2e405abb7a610218168&image=1.png[/img]

So we successfully made an easy anti-anubis function in autoit (:

You can do it just like that in nearly every language.

I know it is possible to make more checks to make a lower chance of a "false positive" but i was just about making an easy one (:

I hope you did enjoy this tutorial,
if you liked it, don't forget to say thanks (:

Warm Regards, Razor

CryptoMatic - November 8, 2012, 6:41 am

very usefull :) I like it
message message

Raz?r - November 8, 2012, 1:38 pm

(Nov 8, 2012 07:41 AM)Rootloot Wrote: [\[CITE\]](#) very usefull :) I like it
message message
Thanks for the feedback.
Glad you like it ?