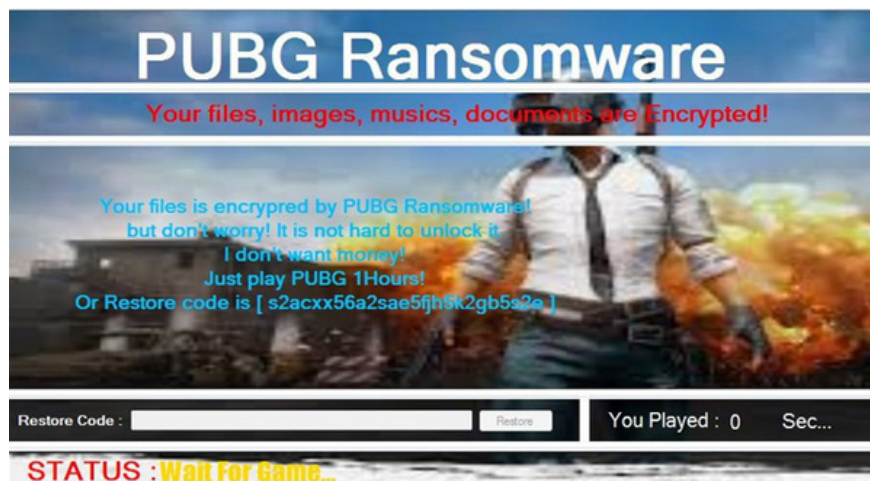


Ransomware appears to require users to play PUBG for 1 hour instead of ransom

PUBG ransomware without ransom requires that players play Bluehole's popular game within an hour to unlock their data.

PUBG ransomware is a new type of ransomware discovered by the MalwareHunter and BleepingComputer teams. Ransomware is special, not only because of the name of this extremely popular game, PlayerUnknown's Battlegrounds (PUBG) but also because it has a different way of operating than other similar malware. PUBG ransomware does not require ransom, it requires players to play this cult game of Bluehole within 1 hour to unlock their data.



But ransomware also provides the unlock code just below for users who don't like or don't have time to play games. Therefore, PUBG ransomware's victims could simply continue to use the device as usual if they just entered the code received.

In addition, although the amount of time required is 1 hour, the data unlocking process will start only 3 seconds after the victim launches the game.

```
Private Sub Timer1_Tick(sender As Object, e As EventArgs)
    Dim processesByName As Process() = Process.GetProcessesByName("TslGame")
    Dim flag As Boolean = processesByName.Length = 0
    'The following expression was wrapped in a checked-statement
    If flag Then
        Me.Label1.Text = "Wait For Game..."
        Me.playtime = Conversions.ToInteger("0")
    Else
        Me.playtime += 1
        Me.may = Me.playtime
        Me.Label1.Text = "You are playing game now!"
        Me.Label4.Text = Conversions.ToString(Me.may)
    End If
    Dim flag2 As Boolean = CDb1(Me.playtime) = Conversions.ToDouble("3")
    If flag2 Then
        Me.Timer1.Stop()
        Dim instance As Object = Strings.Split(MyProject.UserName, "\", -1, CompareMethod.Binary)
        Dim mExtesiones As IEnumerable(Of String) = New String() { ".pubg" }
        Dim ruta As String = Conversions.ToString(Operators.ConcatenateObject(Operators.ConcatenateObject("C:\Users\",
            NewLateBinding.LateIndexGet(instance, New Object() { 1 }, Nothing)), "Desktop"))
        Try
            Dim enumerator As IEnumerator(Of String) = Form1.BuscarArchivos(ruta, mExtesiones).GetEnumerator()
            While enumerator.MoveNext()
                Dim current As String = enumerator.Current
                Form1.RutinaDecifrado(current, "GBUPRansomware", Conversions.ToString(1))
                Me.Encrypted_list.Items.Add("Decrypted : " + current)
            End While
        Finally
            Dim enumerator As IEnumerator(Of String)
            If enumerator IsNot Nothing Then
                enumerator.Dispose()
            End If
        End Try
        Catch expr_167 As Exception
            ProjectData.SetProjectError(expr_167)
            ProjectData.ClearProjectError()
        End Try
        Interaction.MsgBox("Your Files are all Decrypted!!", MsgBoxStyle.OkOnly, Nothing)
        MyBase.Close()
    End If
End Sub
```

This Ransomware monitors the device and searches for information processing called 'TslGame' that occurs when a user starts playing PUBG, regardless of whether the user is actually playing the game or not. Therefore, if you get stuck with this ransomware, the victim can decrypt his data by renaming a certain .exe file to TslGame.exe and start it up.

See more:

1. A series of cult videos, billions of views on YouTube were hacked, renamed and deleted
2. Warning: Detecting more than 1000 Cisco router and switch devices in Vietnam has a serious security error
3. Warning: GandCrab extortionist code is attacking Vietnam
4. Warning of new malware appear like Wannacry, capable of deleting Vietnamese percussion on computer

You finished reading the article "**Ransomware appears to require users to play PUBG for 1 hour instead of ransom**" 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.