Targeted Attack on Government Agencies

By Sushant Kumar Arya, Mohsin Dalla · July 13, 2022

Executive summary

The Trellix Email Security Research Team has discovered a malicious campaign targeting government agencies of Afghanistan, India, Italy, Poland, and the United States since 2021. The attack starts with a spear phishing email with a geo-political theme. The spear phishing emails were themed around India Afghanistan relationship. Attacker used politics as a lure to trick users into clicking on a malicious link. The email used for this phishing attack contains an attachment or a weaponized URL that delivers an Excel sheet. Upon opening the Excel sheet, Excel executes an embedded malicious macro which then decrypts and installs a Remote Access Trojan (AysncRAT & LimeRAT) and maintains persistence. Once the Remote Access Trojan is installed on the victim machine, it establishes communication with a Command-and-Control server used to exfiltrate victim data. The Remote Access Trojan is capable of taking screenshots, capturing keystrokes, recording credentials/confidential information, and adding infected systems to botnets. It can also perform network discovery and move laterally to other systems in the affected organization. The email used in this attack originated from the South Asia region which suggests the involvement of a South Asian threat actor. Trellix Email Security has detection coverage for this malicious campaign.

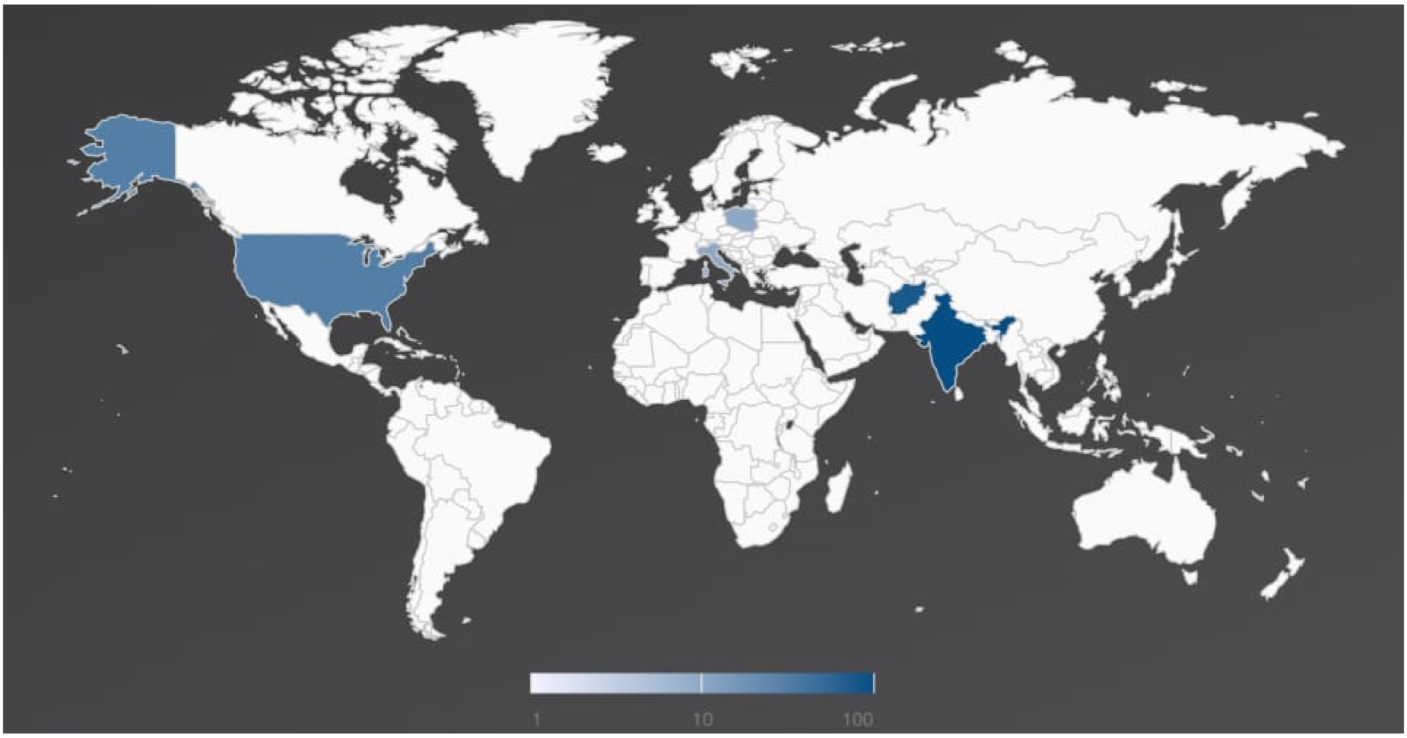


Figure 1. Target countries

Threat landscape

The Trellix Email Security product can follow the entire attack chain and analyze the final payload. In this scenario, it followed the chain: EMAIL -> URL -> ZIP -> XLS -> Macro. Finally, our threat database was able to detect the malicious macro performing decryption, creating an executable object, performing process injection, and utilizing other malicious techniques. Trellix Email Security has detection for the malicious Excel sheet with name - **FE_APT_Dropper_Macro_DoubleHide_1.**

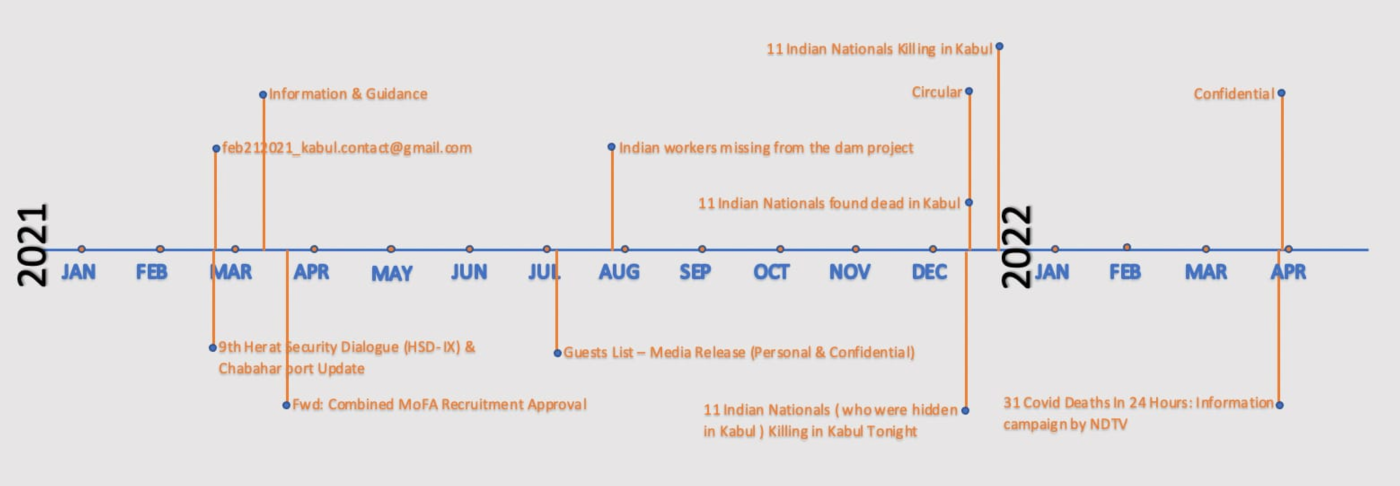


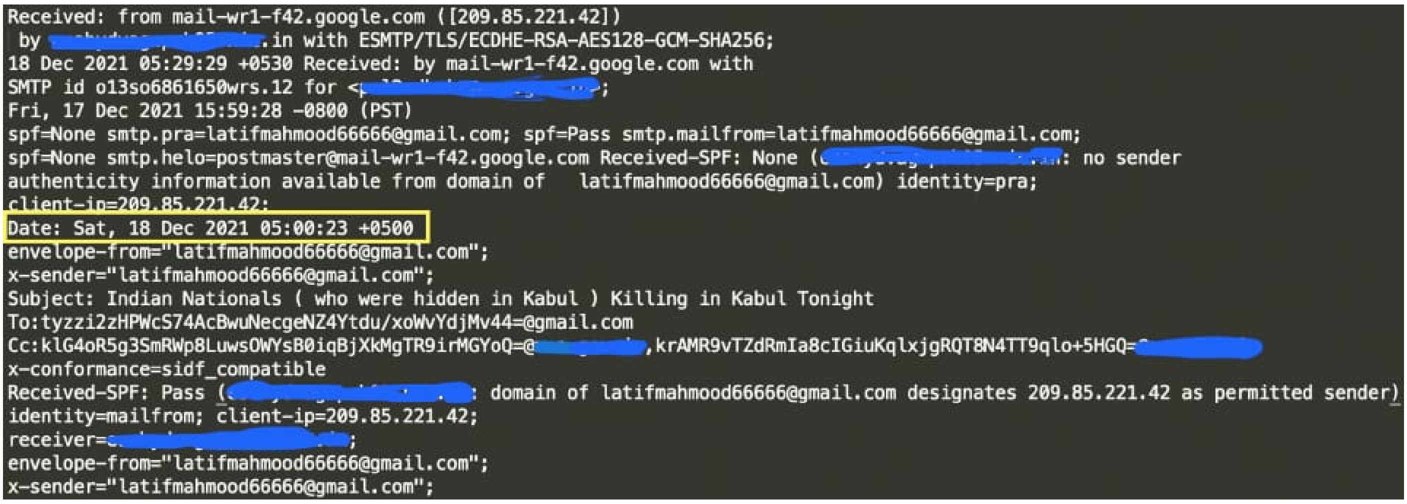
Figure 2. Attack timeline

Attack timeline

As seen in Figure 2, the attack was active for over a year. The attacker sent emails for a short interval and then went back into hiding. This was followed by subsequent similar waves. The first wave of attack was noticed during March-April 2021, followed by another in July 2021, then again in December 2021, and most recently during end of March 2022.

Email details

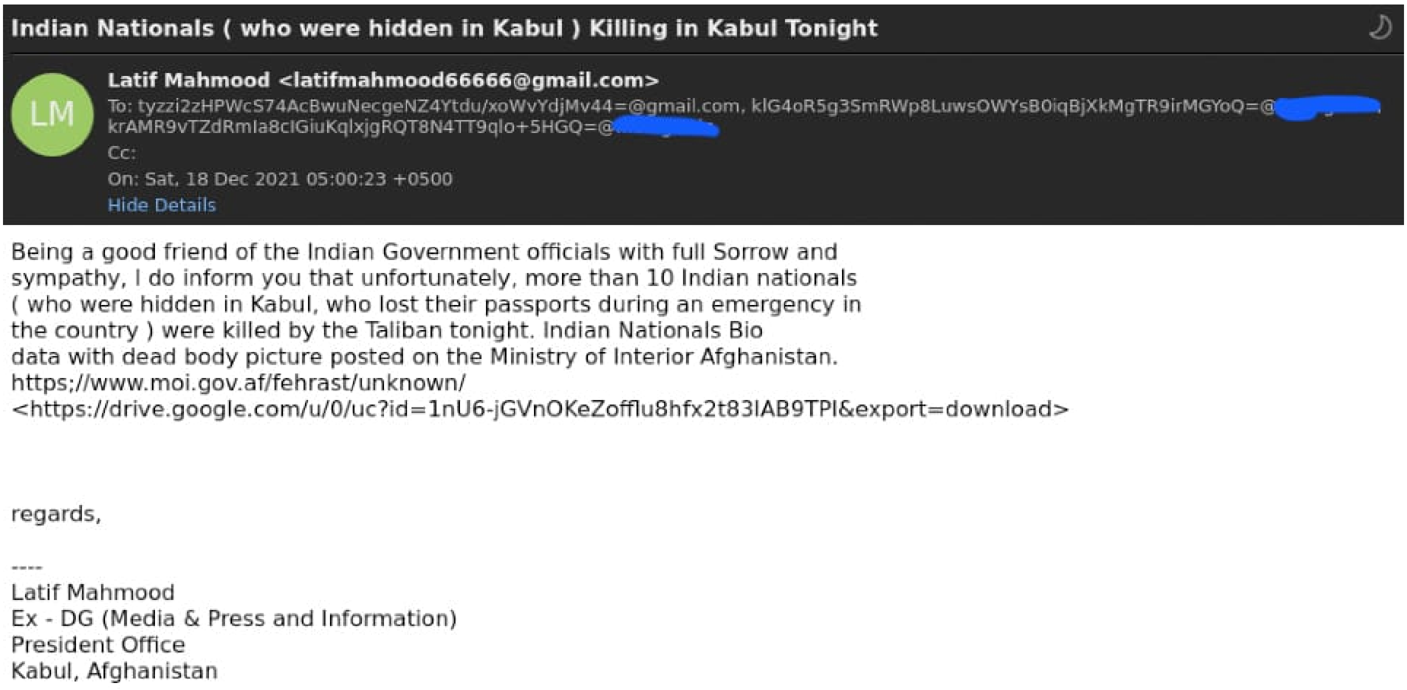
The attackers used the free mail service Gmail to send the spear phishing emails. Based on email header analysis, it was evident that the emails originated from Google servers and were sent from the South Asia region. The time zone of the email sender **(+0500 UTC)** further suggests the involvement of South Asian threat actors.



```
Received: from mail-wr1-f42.google.com ([209.85.221.42])
 by [redacted].in with ESMTP/TLS/ECDHE-RSA-AES128-GCM-SHA256;
18 Dec 2021 05:29:29 +0530 Received: by mail-wr1-f42.google.com with
SMTP id o13so6861650wrs.12 for <[redacted];
Fri, 17 Dec 2021 15:59:28 -0800 (PST)
spf=None smtp.pra=latifmahmood66666@gmail.com; spf=Pass smtp.mailfrom=latifmahmood66666@gmail.com;
spf=None smtp.helo=postmaster@mail-wr1-f42.google.com Received-SPF: None ([redacted]: no sender
authenticity information available from domain of   latifmahmood66666@gmail.com) identity=pra;
client-ip=209.85.221.42;
Date: Sat, 18 Dec 2021 05:00:23 +0500
envelope-from="latifmahmood66666@gmail.com";
x-sender="latifmahmood66666@gmail.com";
Subject: Indian Nationals ( who were hidden in Kabul ) Killing in Kabul Tonight
To:tyzzi2zHPWcS74AcBwuNecgeNZ4Ytdu/xoWvYdjMv44=@gmail.com
Cc:klG4oR5g3SmRWp8LuwsOWYsB0iqBjXkMgTR9irMGYoQ=@[redacted],krAMR9vTZdRmIa8cIGiuKqlxjgRQT8N4TT9qlo+5HGQ=[redacted]
x-conformance=sidf_compatible
Received-SPF: Pass ([redacted]: domain of latifmahmood66666@gmail.com designates 209.85.221.42 as permitted sender)
identity=mailfrom; client-ip=209.85.221.42;
receiver=[redacted];
envelope-from="latifmahmood66666@gmail.com";
x-sender="latifmahmood66666@gmail.com";
```

Figure 3. Email headers

The spear phishing email was themed around geopolitical news related to India like **"Indian Nationals (who were hidden in Kabul) Killing in Kabul Tonight"** and **"Indian workers missing from the dam project."** More recently, the email used a **COVID** theme with the subject **- "31 Covid Deaths In 24 Hours: Information campaign by NDTV".** The email had a Google drive link serving a malicious ZIP file. In some cases, the malicious ZIP was sent as an email attachment. The ZIP contains an Office document which is used to drop a RAT (Remote Access Trojan).



Indian Nationals (who were hidden in Kabul) Killing in Kabul Tonight

LM

Latif Mahmood <latifmahmood66666@gmail.com>
To: tyzzi2zHPWcS74AcBwuNecgeNZ4Ytdu/xoWvYdjMv44=@gmail.com, klG4oR5g3SmRWp8LuwsOWYsB0iqBjXkMgTR9irMGYoQ=@[redacted] krAMR9vTZdRmIa8cIGiuKqlxjgRQT8N4TT9qlo+5HGQ=@[redacted]
Cc:
On: Sat, 18 Dec 2021 05:00:23 +0500

Being a good friend of the Indian Government officials with full Sorrow and
sympathy, I do inform you that unfortunately, more than 10 Indian nationals
(who were hidden in Kabul, who lost their passports during an emergency in
the country) were killed by the Taliban tonight. Indian Nationals Bio
data with dead body picture posted on the Ministry of Interior Afghanistan.
https;//www.moi.gov.af/fehrast/unknown/
<https://drive.google.com/u/0/uc?id=1nU6-jGVnOKeZofflu8hfx2t83IAB9TPI&export=download>

regards,

Latif Mahmood
Ex - DG (Media & Press and Information)
President Office
Kabul, Afghanistan

Figure 4. Email sample

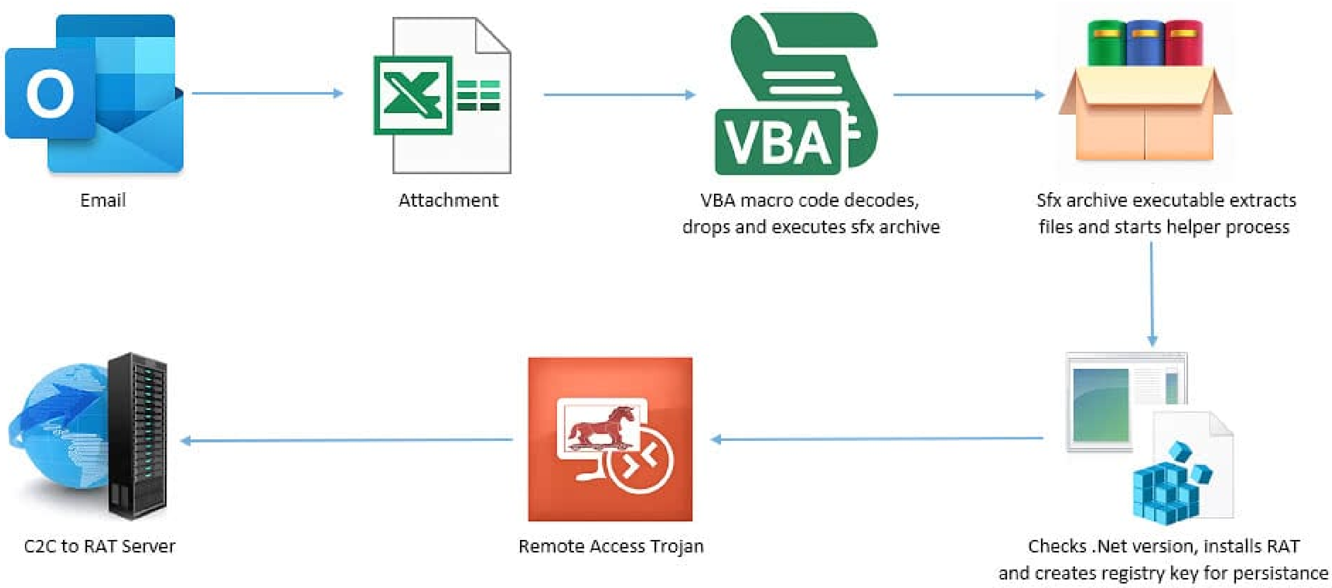
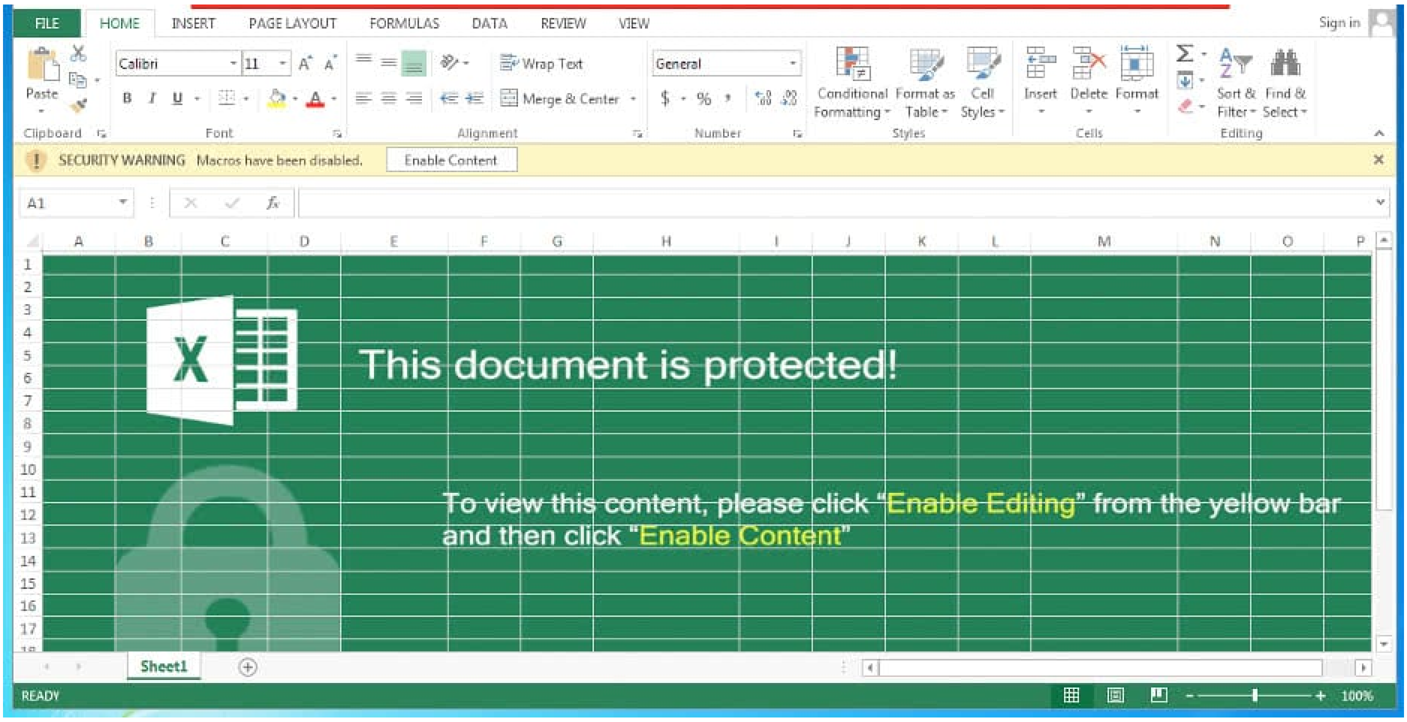

Email
Attachment
VBA
VBA macro code decodes, drops and executes sfx archive
Sfx archive executable extracts files and starts helper process
Checks .Net version, installs RAT and creates registry key for persistance
Remote Access Trojan
C2C to RAT Server

Figure 5. Attack chain

Technical details

The document file (DOC/XLS) acts as a dropper, which drops and executes a file named "msword.exe". The Excel sheet contains a VBA macro which is enabled when the document file is opened. The malicious executable code is stored in the document file itself (within a form text field) in the base64 encoded format. The VBA macro reads the base64 content, decodes it, and then decrypts the decoded content with a hardcoded XOR key. Multiple levels of base64 decoding and XOR decryption are used to obfuscate the malicious executable file.

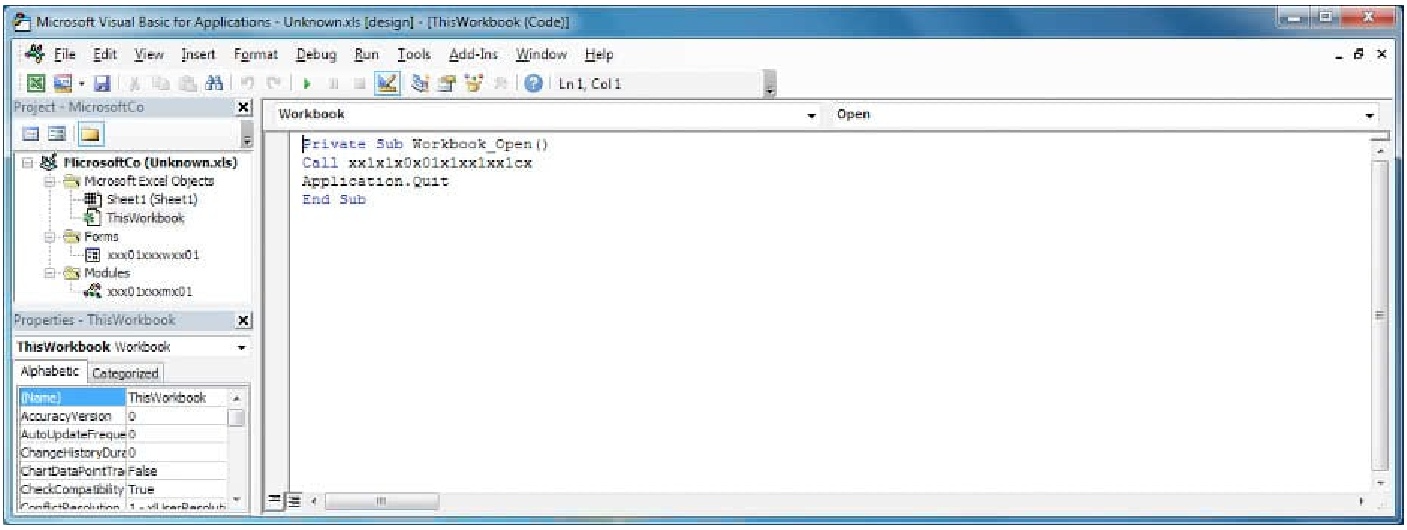


SECURITY WARNING Macros have been disabled. Enable Content

This document is protected!

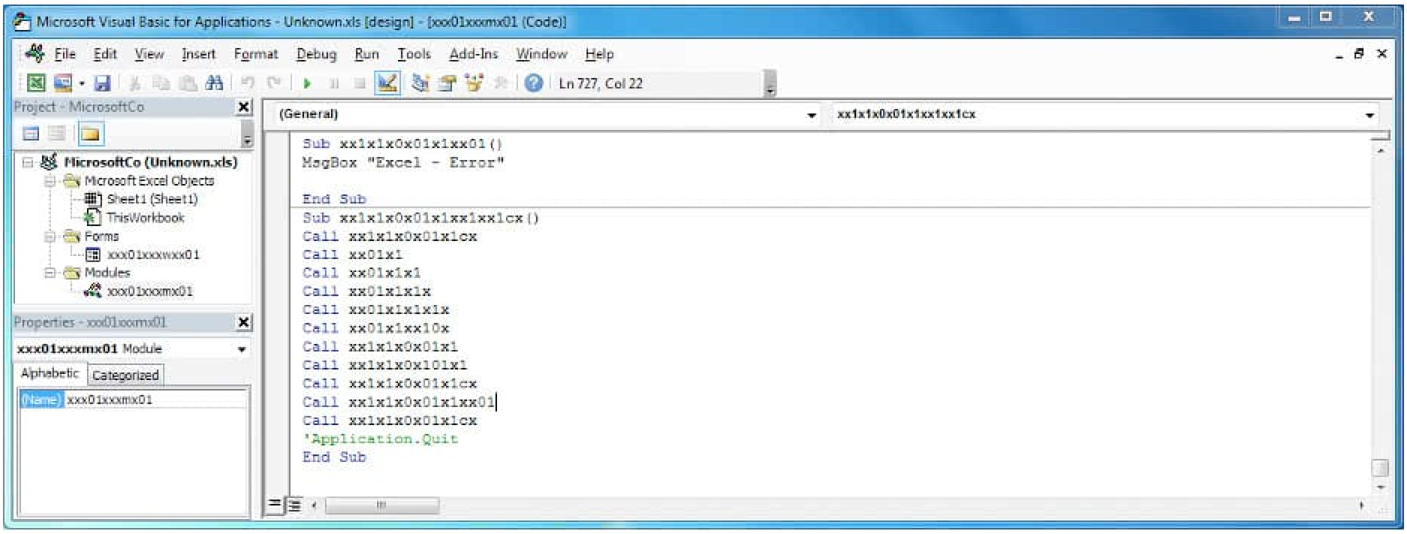
To view this content, please click "Enable Editing" from the yellow bar and then click "Enable Content"

Figure 6. XLS with macro



```
Private Sub Workbook_Open()
Call xx1x1x0x01x1xx1xx1cx
Application.Quit
End Sub
```

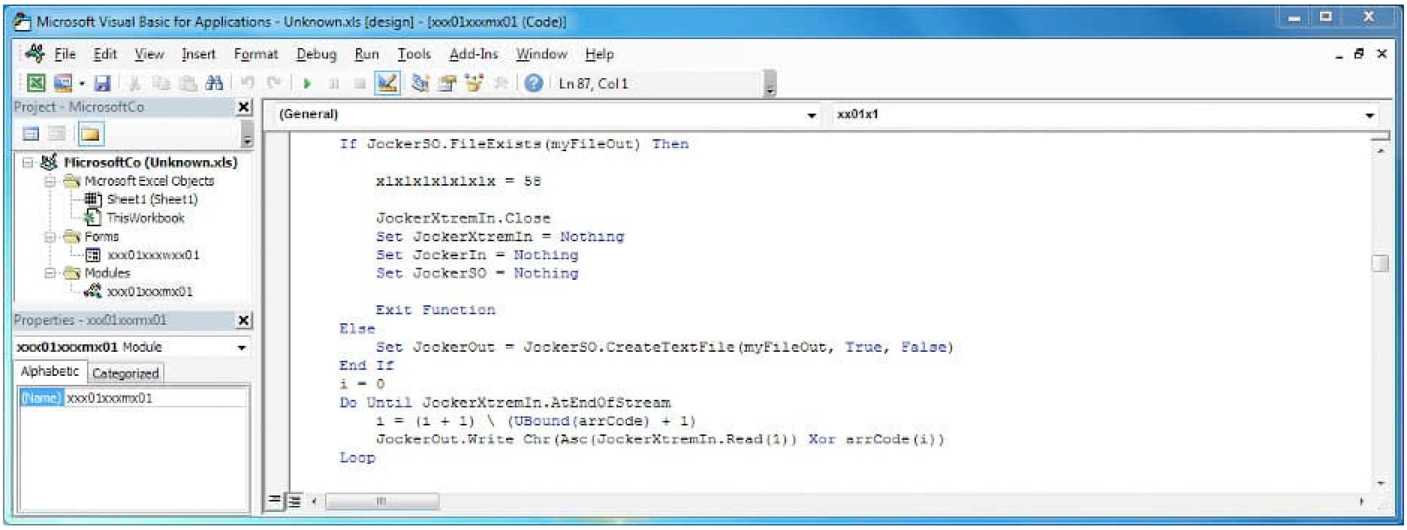
Figure 7. Macro code: Workbook Open



```
Sub xx1x1x0x01x1xx01()
MsgBox "Excel - Error"

End Sub
Sub xx1x1x0x01x1xx1xx1cx()
Call xx1x1x0x01x1cx
Call xx01x1
Call xx01x1x1
Call xx01x1x1x
Call xx01x1x1x1x
Call xx01x1xx10x
Call xx1x1x0x01x1
Call xx1x1x0x101x1
Call xx1x1x0x01x1cx
Call xx1x1x0x01x1xx01
Call xx1x1x0x01x1cx
'Application.Quit
End Sub
```

Figure 8. Macro code: Main function which is called inside Workbook Open event

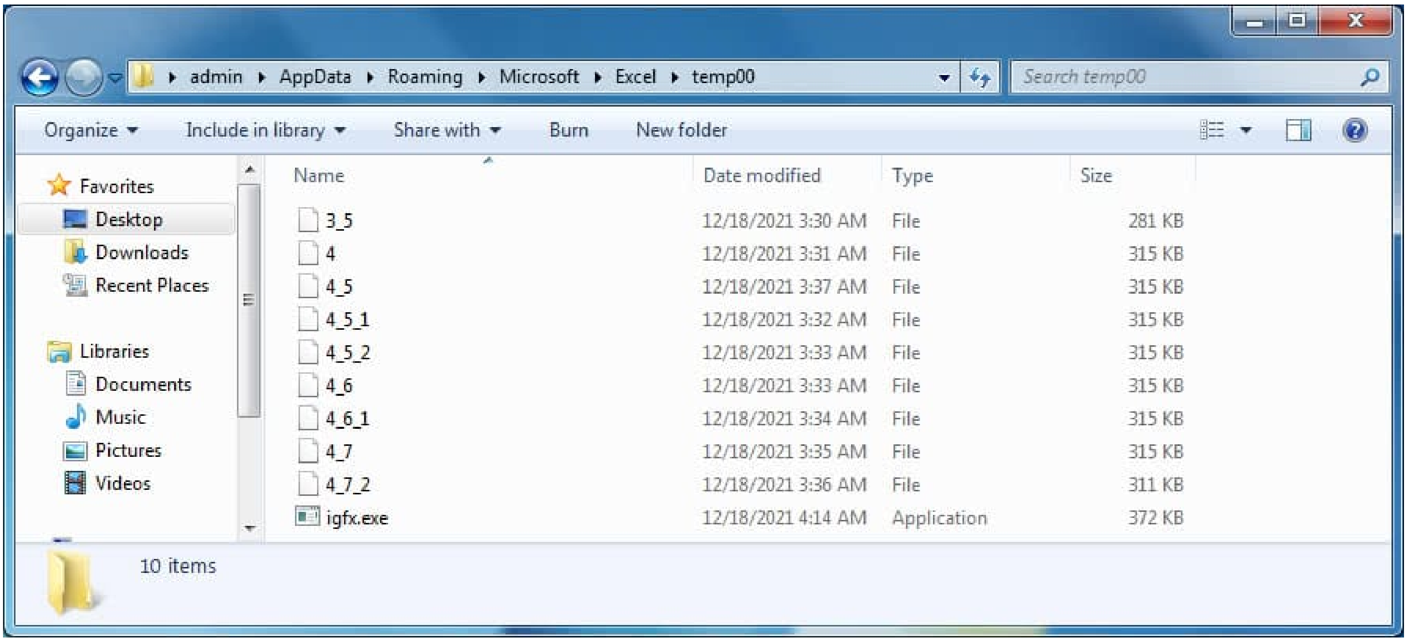
XOR Key :
"MxjnbvbX%$#@c%%!@#$C%^&*(K(*&K0^%W@!&@#$C%EGGGxcel^MicrosoLKHGFD^%$W@2017!&^%$#Ix^&%$0"



```
    If JockerSO.FileExists(myFileOut) Then

        x1x1x1x1x1x1x = 58

        JockerXtremIn.Close
        Set JockerXtremIn = Nothing
        Set JockerIn = Nothing
        Set JockerSO = Nothing

        Exit Function
    Else
        Set JockerOut = JockerSO.CreateTextFile(myFileOut, True, False)
    End If
    i = 0
    Do Until JockerXtremIn.AtEndOfStream
        i = (i + 1) \ (UBound(arrCode) + 1)
        JockerOut.Write Chr(Asc(JockerXtremIn.Read(1)) Xor arrCode(i))
    Loop
```

Figure 9. Macro code: XOR function

“msword.exe” is an SFX archive executable, which contains multiple malicious executable files as shown in Figure 10.



Name	Date modified	Type	Size
3_5	12/18/2021 3:30 AM	File	281 KB
4	12/18/2021 3:31 AM	File	315 KB
4_5	12/18/2021 3:37 AM	File	315 KB
4_5_1	12/18/2021 3:32 AM	File	315 KB
4_5_2	12/18/2021 3:33 AM	File	315 KB
4_6	12/18/2021 3:33 AM	File	315 KB
4_6_1	12/18/2021 3:34 AM	File	315 KB
4_7	12/18/2021 3:35 AM	File	315 KB
4_7_2	12/18/2021 3:36 AM	File	311 KB
igfx.exe	12/18/2021 4:14 AM	Application	372 KB

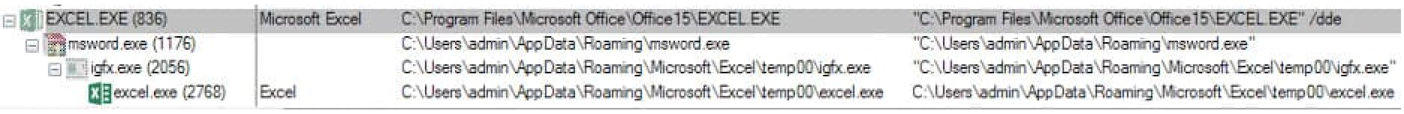
Figure 10. msword.exe contents

File name	File info
3_5	LimeRAT [Runtime: .Net Framework 2.0]
4	AsyncRAT [Runtime: .Net Framework 4]
4_5	AsyncRAT [Runtime: .Net Framework 4.5]
4_5_1	AsyncRAT [Runtime: .Net Framework 4.5.1]
4_5_2	AsyncRAT [Runtime: .Net Framework 4.5.2]
4_6	AsyncRAT [Runtime: .Net Framework 4.6]
4_6_1	AsyncRAT [Runtime: .Net Framework 4.6.1]
4_7	AsyncRAT [Runtime: .Net Framework 4.7
4_7_2	AsyncRAT [Runtime: .Net Framework 4.7.2]
igfx.exe	Delphi compiled file installs RAT file according to available .Net version

Upon execution, "msword.exe" drops the RAT files shown in the table above. These RAT executables are obfuscated using “Crypto Obfuscator For .Net”. “msword.exe” then starts the process “igfx.exe” which performs the following actions:

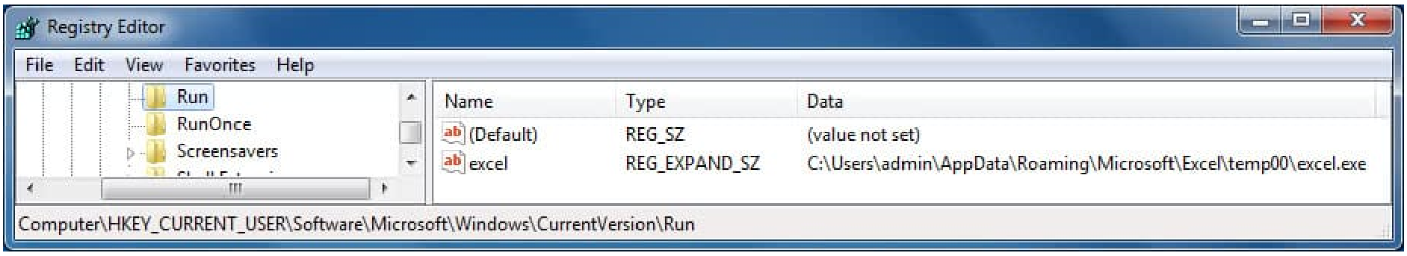
- Checks the .NET version in the registry; based on the installed version, renames the compatible RAT file to “excel.exe”
- Checks the registry keys to determine the .NET version in the order listed below. If found, a version of the runtime file (AsyncRAT) is picked corresponding to the .NET version. If none of the registry keys are found, the file “3_5” (LimeRAT) is used.
  - HKLM\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4
  - HKLM\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4.5
  - HKLM\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4.5.1
  - HKLM\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4.5.2

  - HKLM\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4.6
  - HKLM\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4.6.1
  - HKLM\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4.7
  - HKLM\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4.7.2
- Sets the file attributes of “excel.exe” to hidden and read-only.
- Adds a “Run” registry entry for persistence.
- Deletes the unused RAT executable files.
- Starts the “excel.exe” process.



```
EXCEL.EXE (836)            Microsoft Excel   C:\Program Files\Microsoft Office\Office15\EXCEL.EXE                "C:\Program Files\Microsoft Office\Office15\EXCEL.EXE" /dde
  msword.exe (1176)                          C:\Users\admin\AppData\Roaming\msword.exe                           "C:\Users\admin\AppData\Roaming\msword.exe"
    igfx.exe (2056)                          C:\Users\admin\AppData\Roaming\Microsoft\Excel\temp00\igfx.exe      "C:\Users\admin\AppData\Roaming\Microsoft\Excel\temp00\igfx.exe"
      excel.exe (2768)     Excel             C:\Users\admin\AppData\Roaming\Microsoft\Excel\temp00\excel.exe     C:\Users\admin\AppData\Roaming\Microsoft\Excel\temp00\excel.exe
```

Figure 11. Process chain



Name	Type	Data
(Default)	REG_SZ	(value not set)
excel	REG_EXPAND_SZ	C:\Users\admin\AppData\Roaming\Microsoft\Excel\temp00\excel.exe

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Figure 12. Run registry entries

Both AsyncRAT and LimeRAT source code are publicly available.

Async rat settings configuration

- Ports = "6606”
- Hosts = "107.173.143.111"
- Version = "2.5.7b"
- Install = "false"
- InstallFolder = "AppData"
- InstallFile = "msexcl.exe"
- Key = "MZ-RX
- MTX = "%MTX%";
- Certificate = "%Certificate%"
- Serversignature = "%Serversignature%"
- X509Certificate2 ServerCertificate;
- Anti = "false";
- Aes256 aes256 = new Aes256(Key);
- Pastebin = "null";
- BDOS = "false";
- Delay = "24";
- Group = "Debug";

Async rat commands

- **Server Commands**

pong	Get interval from client
plugin	Run/Load plugin file
saveplugin	Save and Run plugin file

- **Client Commands:**

clientinfo	Send system info to server
ping	Ping server
sendplugin	Get plugin from server

Lime rat settings configuration

- *Pastebin = "https://pastebin.com/raw/DDTVwwbu"*
- *HOST = "107.173.143.111"*
- *PORT = "8989"*
- *EncryptionKey = "MZRX"*
- *ENDOF = "|'N'|"*
- *SPL = "|'L'|"*
- *EXE = "CLIENT.exe"*
- *USB = "false"*
- *PIN = "false"*
- *ANTI = "false"*
- *DROP = "false"*
- *PATH1 = "Temp"*
- *PATH2 = "\Lime\"*
- *fullpath = Environ(PATH1) & PATH2 & EXE*
- *BTC_ADDR = "THIS IS YOUR BTC 1234567890" 'Bitcoin address*
- *DWN_CHK = "true"*
- *DWN_LINK = ""*
- *Delay = "3"*

Lime rat commands

- **Server Commands**

IPSend	Run timer
IP	Stop timer
ICAP	Capture screen Thumbnail
CPL	Check if plugin is installed
IPL	Save plugin and then load it (server send plugin)
IPLM	Load plugin without saving it (server send plugin)

- **Client Commands**

INFO	Sends system info
IP	Ping to server
IPStart	Timer started
#CAP	Sending Thumbnail
GPL	Get plugin from server
MSG	Send Message

These RATs can extend their capabilities using existing or user-defined plugins. At the time of analysis both AsyncRAT and LimeRAT were not getting responses from the C2 server “107.173.143.111”

Detections and Indicators

FE_APT_Dropper_Macro_DoubleHide_1

MITRE ATT&CK Techniques

T1071	Application Layer Protocol	HTTP/DNS requests are used in the C&C traffic
T1036	Masquerading	The registered task/service pretends to be benign by name
T1056	Input Capture	Keylogging capabilities
T1113	Screen Capture	Can capture the screen of the victim
T1115	Clipboard Data	Collect data stored in the clipboard from users copying information within or between applications.
T1049	System Network Connections Discovery	Performs network discover for lateral movement into network
T1547	Boot or Logon Autostart Execution	Run entry is made when persisting via the registry
T1204	User Execution	Opening malicious xls to execute macro
T1041	Exfiltration Over C2 Channel	Send stolen data using CNC channel
T1137	Office Template Macros	Execute malicious code upon macro execution

IOCs:

File Name	SHA256
3_5	7a6b87a7ba79160232579157b8ebcaea7660392d98cb6b8b3d562a383a0894bc
4	5e44f769aa9a745ade82589bbbd17c3687f2fb7c08b1043d8c5c44d28eaa20a9
4_5	fe1c8b01f5abc62551b0a3f59fe1675c66dd506d158f5de495a5d22d7445e6e9
4_5_1	fa9cb5608841f023052379818a9186496526039bc47cac05a6866f5fb0e70fc5
4_5_2	080fcc70c11248eaf34bd30c0dc9800b0b1742fe92c96c9995a1c73c0adf2336
4_6	465a59b7a97364bc933703a8fda715090c6a927f814bc22a0057e6a7134cb69f
4_6_1	5e082d1c85e591aebb380d7d7af56000ac0ef5fc32e216cb5fe7027bb9861743
4_7	f59dc209ee236e5ed78f83117865164e57a223f742c75f57c20d3da4cbe179e0
4_7_2	f32b0d71274ea93f27527079371e5e926e8d6a6f29d84ac602e48da0332c9f4c
igfx.exe	8248432bcba6e8bb8731c0b8f2fbe4aae2e2d0fee2157477c83343743c39c1a8

msword.exe	06064b3b0158efbfa9d849c853a9783c7e9d07c5924275d0d33c6ac74c78eec7
Unknown.xls	886c5883113d279d97caaca2714860dfceb421c7297dbb3ee04a00b7d50b821b
Unknown.ZIP	b9584cf67e73a759d6c412962d4a9d7471c703f72e056cd24742a4b78c68ff2d

URL:hxxps://drive.Google.com/u/0/uc?id=1nU6-jGVnOKeZofflu8hfx2t83lAB9TPI&export=download
CnC:107.173.143.111

Email Subjects:

9th Herat Security Dialogue (HSD- IX) & Chabahar port Update
feb212021_kabul.contact@gmail.com
Information & Guidance
Fwd: Combined MoFA Recruitment Approval
Guests List - Media Release (Personal & Confidential)
Indian workers missing from the dam project
Indian Nationals (who were hidden in Kabul) Killing in Kabul Tonight
11 Indian Nationals found dead in Kabul
Circular
Indian Nationals Killing in Kabul
31 Covid Deaths In 24 Hours: Information campaign by NDTV

Email Senders:

kabul.contact@gmail.com
mashrefhaideri@gmail.com
latifmahmood66666@gmail.com
fscon.kab@gmail.com
admn.kabul@gmail.com
ravish49.ndtv@gmail.com